Calhoun
Institutional Archive of the Naval Postgraduate School

Calhoun: The NPS Institutional Archive

DSpace Repository

Theses and Dissertations | 1. Thesis and Dissertation Collection, all items

2003-12

Confronting cyberterrorism with cyber deception

Tan, Kheng Lee Gregory

Monterey, California. Naval Postgraduate School

http://hdl.handle.net/10945/6132

Copyright is reserved by the copyright owner

Downloaded from NPS Archive: Calhoun

http://www.nps.edu/library

Calhoun is the Naval Postgraduate School's public access digital repository for research materials and institutional publications created by the NPS community. Calhoun is named for Professor of Mathematics Guy K. Calhoun, NPS's first appointed -- and published -- scholarly author.

Dudley Knox Library / Naval Postgraduate School
411 Dyer Road / 1 University Circle
Monterey, California USA 93943

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

CONFRONTING CYBERTERRORISM WITH CYBER DECEPTION

by

Kheng Lee Gregory Tan

December 2003

Thesis Advisor:	Neil C. Rowe
Second Reader:	Dorothy E. Denning

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** December 2003	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: Confronting Cyberterrorism with Cyber Deception		**5. FUNDING NUMBERS**	
6. AUTHOR Kheng Lee Gregory Tan			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE**	

13. ABSTRACT (maximum 200 words)

This thesis concerns the possibility of deceiving cyberterrorists using defensive deception methods. As cyberspace today is a battleground for myriad cyber attacks and intrusions, it may only be a matter of time before terrorists choose to advance their deadly cause in cyberspace. We explore some of the questions raised regarding the threat of cyberterrorism by examining different perspectives, motivations, actors, targets, and how they may be confronted. One way is to draw from the lessons of deception and apply them against cyberterrorist attacks. Cyber deception applies in cyberspace just as well as deception in military battles. From the different categories of attackers that could perpetrate cyberterrorism, we examine the ways in which they may be deceived. Many of the methods and tools that cyberterrorists would use are similar to those used by other less malicious hackers, so we can plan specific deceptions to use against them in advance.

14. SUBJECT TERMS Information warfare, terrorism, cyberterrorism, deception, intelligent software decoys, computer deception			**15. NUMBER OF PAGES** 87
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

CONFRONTING CYBERTERRORISM WITH CYBER DECEPTION

Kheng Lee Gregory Tan
Lieutenant-Colonel, Singapore Army
B.Eng, University College London, 1990

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

from the

NAVAL POSTGRADUATE SCHOOL
December 2003

Author: Kheng Lee Gregory Tan

Approved by: Neil C. Rowe
Thesis Advisor

Dorothy E. Denning
Second Reader

Peter J. Denning
Chairman, Department of Computer Science

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This thesis concerns the possibility of deceiving cyberterrorists using defensive deception methods. As cyberspace today is a battleground for myriad cyber attacks and intrusions, it may only be a matter of time before terrorists choose to advance their deadly cause in cyberspace. We explore some of the questions raised regarding the threat of cyberterrorism by examining different perspectives, motivations, actors, targets, and how they may be confronted. One way is to draw from the lessons of deception and apply them against cyberterrorist attacks. Cyber deception applies in cyberspace just as well as deception in military battles. From the different categories of attackers that could perpetrate cyberterrorism, we examine the ways in which they may be deceived. Many of the methods and tools that cyberterrorists would use are similar to those used by other less malicious hackers, so we can plan specific deceptions to use against them in advance.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION 1

II. CYBERTERRORISM 5
- A. ORIGINS OF TERROR 5
  - 1. Defining Terrorism 6
  - 2. Motivations of Terrorism 8
  - 3. Terrorists and Cyberspace 9
- B. WHAT IS CYBERTERRORISM? 11
  - 1. Defining Cyberterrorism 12
  - 2. Cyberterrorist "Camps" 14
- C. THE CYBERTERRORISM THREAT 17
  - 1. Motivations 17
  - 2. Actors 18
  - 3. Targets 20
  - 4. Understanding the Threat 22
  - 5. Combating the Threat 23

III. DECEPTION 25
- A. THE MANY FACES OF DECEPTION – DECEPTION IN ACTION 25
  - 1. Deceptions in Nature 25
  - 2. Deceptions in Human History 26
- B. DEFINING DECEPTION 28
  - 1. Taxonomy of Perception 29
  - 2. Structure of Deception 30
- C. THE VALUE OF DECEPTION 31
  - 1. For the Attacker 31
  - 2. For the Defender 31
  - 3. Nesting Deceptions 32
- D. THE DECEPTION PLANNING PROCESS 33
- E. DECEPTION, INTELLIGENCE AND COUNTER-DECEPTION 34
- F. PITFALLS OF DECEPTION 35
  - 1. Traps That Backfire 35
  - 2. Active and Passive Deception 36
  - 3. Legalities 36

IV. CYBERTERRORISTS AND CYBER DECEPTION 39
- A. DECEPTIONS IN CYBERSPACE 39
- B. THEORY OF CYBER DECEPTION 42
  - 1. A Taxonomy of Cyber Deception 42
    - *a. Concealment 42*
    - *b. Camouflage 43*
    - *c. False and Planted Information 43*
    - *d. Ruse 44*

e. Display 44
f. Demonstration 44
g. Feints 45
h. Lies 45
i. Insight 46
2. Semantic Cases 46
C. CYBER DECEPTION AND CYBER DEFENSE 48
1. Software Decoys 48
2. Other Related Work 50
D. PITFALLS OF CYBER DECEPTION 51
E. CYBERTERRORISTS AND CYBER DECEPTION 52
1. Attack Tools 52
2. Terrorists, Cyberterrorists, and Deception 55
V. CONCLUSION 61
LIST OF REFERENCES 63
INITIAL DISTRIBUTION LIST 71

LIST OF FIGURES

Figure 1. A Taxonomy of Perception (After [Whaley, 1982]) 29
Figure 2. Software Decoy Architecture (From [Michael et al, 2002]) 49

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1. The Structure of Deception (After [Whaley, 1982]). 30
Table 2. A Selected List of Semantic Cases as Applied to Information Systems (After [Rowe, 2004]). 47
Table 3. Cyberterrorism Techniques (After [Denning1, 1999; Dunnigan, 2002; Fox et al, 2002]). 53
Table 4. Cyberterrorism Attack Tools (After [Cohen1, 1998; Denning1, 1999]). 54
Table 5. Deceptions against Cyberterrorists. 58
Table 6. Cyber Deceptions and Cyber Attacks 59

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to thank Dr Neil Rowe and Professor Dorothy Denning for inspiring me to embark on this work. In particular, I would like to thank Dr Rowe for his guidance, encouragement and support throughout the past six months, and Professor Dorothy Denning for her ideas and inputs as I developed the thesis.

This work is dedicated to my wife, Simone, for her prayers, love, support, encouragement, and for managing the home while I toiled away in the study; to my two sons, Jonathan and Joseph, who were a constant source of motivation, joy, and distraction over the past year.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

Much has been written about an “Electronic Pearl Harbor” even before the attacks on September 11, 2001 in New York and Washington D.C. In the aftermath of the attacks, even more questions have been raised about the possibility and probability of terrorist attacks in cyberspace following suit. As it is, the Carnegie-Mellon Computer Emergency Response Team Coordination Center (CERT/CC) has documented nearly 300,000 Internet security incidents since 1988, with nearly two-thirds of them occurring between 2002 and the first three quarters of 2003 [CERT, 2003]. The culprits behind these incidents are not always evident, but often they are the work of hackers, malicious programmers, script kiddies and the like. Instead of these types of perpetrators, the person responsible could belong to a cyberterrorist group which has express intentions to inflict some form of widespread damage to further its cause.

The irony of the historical Pearl Harbor is that, while the operation was a spectacle of military deception, coordination and resource management, the executor of the operation, the Imperial Japanese Navy, was decimated in the years that followed it. The attacker’s success was short-lived. Indeed, some are now suggesting that the threat of an “electronic Pearl Harbor”, in which a crippling blow is inflicted against national information systems, financial institutions, and so on, is not as significant as that of an “electronic Waterloo”, which would entail the long-term and systematic alteration of the world’s political, military and economic order. In this case, the attackers could conduct covert reconnaissance for months if not years to ascertain critical information assets to be targeted or exploited before the execution of the actual operations [CSIS, 1998].

The continuing increase in reported Internet incidents probably stems from the growth of the Internet in recent years. The Internet counts among its consumers genuine users as well as those who would seek to exploit it for unscrupulous means or do harm. The increasing complexity of software such as

operating systems and Web browsers increases security vulnerabilities. At the same time, hacking tools are also increasing in sophistication and availability, meaning that vulnerabilities once exposed are quickly exploited [Denning, 2001]. U.S. Department of Defense surveys also showed that cyber incidents including probes, illicit entry and attacks aimed at causing damage and taking control have been on the rise, somewhat corresponding to the increasing availability of hacking tools, discoveries of vulnerabilities in software, and the growth of the Internet [Ashley, 2003]. To protect genuine users from "others", various measures have been explored including law enforcement, deterrence, protection mechanisms, self-defense, consumer education, and awareness. In this thesis, one particular protection mechanism is examined, that of software deception.

Before proceeding, we briefly explain the key concepts used in the subsequent chapters and how they relate to one another. These key concepts fall under the topic of Information Operations (IO). While there are several definitions of IW, the one from the U.S. Department of Defense will be taken as representative:

> Information Warfare includes actions taken to preserve the integrity of one's own information system from exploitation, corruption, or disruption, while at the same time exploiting, corrupting, or destroying an adversary's information system and in the process achieving an information advantage in the application of force [Joint, 1995].

In the definition above, one part deals with the offensive aspect of IW. In cyberspace, this would involve attacks on the confidentiality and integrity of data or the availability of services. Examples would include the insertion of malicious code such as Trojan horses, viruses or worms into the target computers, servers, or networks, the penetration of the targets to secure unauthorized access to data, or the execution of flood attacks to deny services. These would be classified as cyber attacks. Many of the techniques and tools that could be employed in cyberterrorism are those used in cyber attacks, and thus fall into the offensive IW category. Another part of the definition deals with the defensive aspect of IW. In

cyberspace, this involves the protection of data confidentiality and integrity, and ensuring and sustaining availability of services. Examples include the use of encryption to protect data, implementation of firewalls, and use of intrusion detection systems to prevent or detect unauthorized intrusions. Defensive IW also includes cyber deception, the use of deception techniques to fool or foil cyber attacks. The use of deception in software defenses thus falls under the category of defensive IW [Denning1, 1999; Waltz, 1998].

The next chapter discusses terrorism as the root of cyberterrorism. The difficulty in defining terrorism has created different ideas of what cyberterrorism could be. We explore the makeup and motivations for terrorism to see how they subsequently lend themselves to cyberterrorism. In the discussion on cyberterrorism, different perceptions are considered in an attempt to find principles of the threat posed by cyberterrorism. In doing so we discuss the motivations, actors and targets of cyberterrorism. Various measures that have been adopted to combat the threat of cyberterrorism are also discussed.

Chapter III explores the use of deception in human history and in cyberspace. Various aspects of deception are examined, such as the structure, value and risks associated with the practice of deception. We also explore the aspects of deception most related to terrorism, namely intelligence and counter-deception.

Chapter IV examines the use of deception in cyberspace and how these relate to deceiving cyberterrorists. Different theories of cyber deception are discussed and provide the basis for an examination of several works on the use of cyber deception in defense of information systems. We also explore the possible attack tools that cyberterrorists would use. These are then tied in with discussions on the means by which cyberterrorists may be deceived in defense of information systems.

Chapter V concludes by summarizing the key issues and conclusions drawn in this thesis and postulates areas for future work.

THIS PAGE INTENTIONALLY LEFT BLANK

II. CYBERTERRORISM

A. ORIGINS OF TERROR

Act of Terrorism = Peacetime Equivalent of War Crime

Alex P Schmid (1992)

Although terrorism is one of the most ubiquitous words in the current affairs, political or conflict news of the present day, few agree on exactly what is terrorism. As the famous cliché goes: one man's terrorist is another man's freedom fighter. Hence, terrorists never call themselves as such, and will go to great lengths to evade such connections [Hoffman, 1999].

Arguably, and unsurprisingly, the roots of terrorism could be found in religion, during the Middle East of the 1st Century [Reich, 1998]. The Sicarii were an active Jewish group which set out to target other Jews who collaborated with the Romans. The Zealots were also a Jewish group that targeted the Romans and Greeks. These executions would typically be carried out in broad daylight in the presence of others. The objectives for such action were in part to inspire insurrection among the Jews against the Roman occupiers, and in part to send a message to the Roman authorities themselves. In his study of terrorism, [Hoffman, 1999] showed how the understanding and perception of terrorism changed over the centuries. Terrorism was popularized during the French Revolution toward the end of the 18th Century with the *régime de la terreur,* which gave us the English word "terror". It had then a positive connotation as it was the system by which order was established during an anarchical period in France. Over time, however, its use became associated with anti-monarchy, anarchy, revolution, anti-establishment, violence and anti-government activity. The modern meaning of the word only emerged after the Second World War when terror was used to describe the anti-colonialistic, nationalistic and separatist revolts that were typically violent.

1. Defining Terrorism

An expert on terrorism, Alex P. Schmid, made an attempt to provide a broad definition of terrorism when he examined over a hundred definitions in 1984, and came up with 23 different characteristics that appeared in these definitions. The five most frequently occurring ones were (1) violence and force; (2) political; (3) fear and terror emphasized; (4) threat; (5) (psychological) effects and (anticipated) reaction. The United Nations in the 1970s tried in vain to come to an agreement on what was and what was not terrorism. Many of its members held the view that struggles against occupation or oppression, or struggles for liberation, freedom or independence, even if they include acts of violence, should not be considered as terrorism [Hoffman, 1999]. Fueling the debate further is the media, who have been inconsistent in their description of events. [Crenshaw, 1995] suggested a reason for the difficulty in defining terrorism is that terrorism is a political label. Thus to label a group or act as "terrorist" effectively places a moral judgement on it, denies it political status, acceptance or recognition, and frames the consciousness of the masses.

In the light of the many events since the 1970s that involved all if not more than the five characteristics mentioned, the United Nations Office on Drugs and Crime (UNODC) has since adopted an academic consensus definition provided by Alex P. Schmid in 1988:

> Terrorism is an anxiety-inspiring method of repeated violent action, employed by (semi-) clandestine individual, group or state actors, for idiosyncratic, criminal or political reasons, whereby – in contrast to assassination – the direct targets of violence are not the main targets. The immediate human victims of violence are generally chosen randomly (targets of opportunity) or selectively (representative or symbolic targets) from a target population, and serve as message generators. Threat- and violence-based communication processes between terrorist (organizations), (imperiled) victims, and main targets are used to manipulate the main target (audience(s)), turning it into a target of terror, a target of demands, or a target of attention, depending on whether intimidation, coercion, or propaganda is primarily sought.

The short legal definition proposed by the same author in 1992 defined an act of terrorism as “the peacetime equivalent of a war crime”, since it is generally agreed that terrorists are known by a refusal to be bound by international rules of warfare and codes of conduct. However, the validity of this short form is now somewhat uncertain with a blurring of the lines between wartime and peacetime actions, especially with “the war against terror” undertaken by the U.S. military and its allies in Afghanistan and now Iraq. The U.S. Homeland Security Act of 2002 defined terrorism as follows:

> The term “terrorism” means any activity that—
> (A) involves an act that—
> (i) is dangerous to human life or potentially destructive of critical infrastructure or key resources; and
> (ii) is a violation of the criminal laws of the United States or of any State or other subdivision of the United States; and
> (B) appears to be intended—
> (i) to intimidate or coerce a civilian population;
> (ii) to influence the policy of a government by intimidation or coercion; or
> (iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping.

The agencies of the U.S. government continue to provide their own definitions of terrorism, each reflecting their organizational characteristics and focus:

> The unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives. (U.S. Federal Bureau of Investigation)
>
> The calculated use of violence or the threat of violence to inculcate fear, intended to coerce or intimidate governments or societies as to the pursuit of goals that are generally political, religious or ideological. (U.S. Department of Defense)
>
> Premeditated, politically motivated violence perpetuated against noncombatant targets by subnational groups or clandestine agents, usually intended to influence an audience. (U.S. State Department)

2. Motivations of Terrorism

There are probably as many motivations for terrorism as there are definitions. The three most common motivations are political, religious, and ideological. Of these, political motivation is the most prominent as it features in most definitions of terrorism. [Crenshaw, 1981] suggested that the direct causes of terrorism are unjust discrimination, a lack of opportunity for political participation, élite dissatisfaction, and precipitating events. The first factor stems from grievances experienced by one subgroup in the population, such as an ethnic minority, due to unequal rights or the desire to gain a separate, independent state. Grievances alone do not generate terrorist reactions, but they are more likely to occur if the discriminations are deemed to be unjust, and if violence is considered as a viable means to redress the situation. Regimes that suppress opportunities for political participation, either by denying access to power or by persecuting dissidents, are bound to create dissension. In such situations are the seeds for revolutionary terrorism sown. Terrorism is also likely to occur when the young élite find themselves at odds with society and its general passivity. Student unrest is one such example of élite dissatisfaction, and may lead on to terrorist incidents. The last factor cited by Crenshaw derives from instances such as the use of unexpected and unusual force in response to protest or reform attempts by the government. This excessive use of force has created notable terrorist groups, such as the Irish Republican Army (IRA) and the Red Army Faction (RAF) of West Germany.

Although the September 11 attacks were confined to New York and Washington D.C., airport security was immediately tightened not just in the U.S. but also in many parts of the world. As acts of political violence, the ramifications extend beyond the immediate target of violence, usually affecting the wider audience of the local population, and in many instances across national borders. This wide-reaching impact of terrorism serves as a strong motivation for terrorists [Post, 1998]. A terrorist group also needs to commit acts of violence as that has become what is necessary for the group to justify its existence. At the same time, it will deliberately steer away from any claims of success in achieving its

espoused causes. This avoidance of success is paradoxical – while the objective is the cause, success can take it away, as once a terrorist group has achieved its objective, it would have nothing left to fight for.

[Whittaker, 2001] cites three other possible motivations of terrorism: rational, psychological and cultural. The rational motivation requires a business-like approach which considers cost-benefit analysis and risk analysis as a critical part of the thought process. An error of judgement could lead to the demise of the group itself. Psychological motivation encompasses the true believer of a cause, one who needs to belong to a group. At the same time, the group imposes a polarized “us versus them” outlook, with “them” as the evil ones, thereby justifying any violent action taken by the group. Moreover, a terrorist group must terrorize, if anything else to ensure continued self-esteem and worthiness of their label. Motivations for the cultural category deal with responses to threats against ones own existence. If a people feel that their ethnicity, religion, culture, language or even way of life is being suppressed or threatened by external influences, they may be prepared to resort to actions amounting to violence to ensure their survival. This will be especially so if their perception of the threat is such that they think it will capitulate in the face of violent action, they will press ahead to the results that they seek.

3. Terrorists and Cyberspace

Web sites are posted by various terrorist groups for specific purposes. Some like jehad.net and aloswa.org were set up by Al Qaeda supporters to show support for Osama bin Laden, while others like 7hj.7hj.com teach the use of hacking to serve Islam [Ashley, 2003]. The Hizbullah were known to operate three sites as at February 1998: hizbullah.org served as the central press office, moqawama.org described its attacks against Israel, and almanar.com.lb provided news and information [Denning1, 2000]. Many others are listed in [Thomas 2003], the most notable of which is alneda.com which features international news on Al Qaeda, and purportedly contains encrypted information leading to more secure sites. [Thomas, 2003] also describes the use of the Internet for cyberplanning to support the terrorist cause through Web publicity, propaganda,

research and information gathering, recruitment, planning and coordination. Specific activities include the use of the Internet for profiling, hiding identities, raising money, recruiting, information gathering, disrupting businesses, as well as for command and control, communications, propaganda and mobilization.

Initiating attacks in cyberspace may be a natural progression for terrorists. The final instructions from Mohammed Atta before the September 11 carnage reportedly went as follows [Thomas, 2003]:

> The semester begins in three more weeks. We've obtained 19 confirmations for the studies in the faculty of law, the faculty of urban planning, the faculty of fine arts, and the faculty of engineering.

In hindsight, one can now postulate that the 19 "confirmations" refer to the hijackers and the 4 faculties mentioned could either refer to the 4 aircraft to be used in the attack, or the 4 targets.

The value of the Web is so well acknowledged that almost every known terrorist group has a Web site. They cannot even be forced off, as they can either go to countries with broad free-speech laws, or take advantage of service providers who are unaware of their existence. For example, alneda.com was first hosted in Malaysia, subsequently in Texas and then Michigan, before being shut down in June 2002 [Denning1, 2000; Thomas, 2003].

Electronic mail alongside cell phone surveillance has provided the U.S. FBI and CIA with valuable Intelligence. Reportedly, many Al Qaeda trainees were lax when it came to operational security pertaining to electronic mail and cell phones. Added to that was the use of the weaker 40-bit encryption or no encryption at all in their electronic mail or stored electronic documents, exposing them to eavesdropping and capture [Dunnigan, 2002]. In spite of these setbacks, it is evident that electronic mail – encoded, encrypted or otherwise – is a critical component of communications for many terrorist groups.

B. WHAT IS CYBERTERRORISM?

> Cyberterrorism is the convergence of cyberspace and terrorism.
>
> Dorothy E. Denning (2000)

On October 21, 2002, in what was touted as "the most sophisticated and large-scale assault against these crucial computers in the history of the Internet", nine out of the Internet's thirteen core domain name servers were attacked for an hour with an overwhelming stream of traffic, effectively shutting them down. Fortunately, there was no appreciable impact on the Internet itself since the critical information stored on those domain name servers was cached in thousands of other servers around the world [Sullivan, 2002; Wired News, 2002]. But immediately after the attack, some warned that larger attacks were in the pipeline, and questioned if the Internet infrastructure was adequately robust to withstand similar if not worse attacks in future.

In September 2003 the Al-Farouq Web site, which is purported to be directly affiliated to Osama bin Laden's Al Qaeda, published a book on one of its Web sites entitled "The 39 Principles of Jihad", or more specifically, the 39 principles of *Al Qaeda's* Jihad. Jihad, which literally means a struggle in the name of God, is also closely associated with holy war. This is reflected in the "39 Principles". What is of particular interest are calls for followers to utilize the availability of modern technology to spread the message of their cause, including Internet Web sites and forums, and telecommunication tools such as SMS (smart messaging systems). In addition, the followers were called to "Perform electronic Jihad" by making use of their skills to "destroy American, Jewish and secular Web sites as well as morally corrupt Web sites" [Leyden, 2003].

These examples illustrate the problems in dealing with cyberterrorism. In the first example, denial-of-service attacks showed that while there were those who sought to disrupt if not disable the Internet, the identity of the perpetrators

and the real motives behind the attack were unknown. Was it the work of several teenage whiz kids out to test their cyber skills, or a group of terrorists seeking to further their cause? Nor was it clear why the attacks came to a sudden halt after an hour. Some speculated that this was only a test run and that larger attacks are to be expected. Others suggested that the attackers stopped after realizing that the attacks did not have the intended effect. Perhaps it was the work of some good Samaritans who wanted to send a warning sign to the DNS operators to secure their systems properly, since that was what several of the operators have done following the incident [Wired News, 2002]. In the second example, one of the most notorious terrorist groups today is advocating the use of cyberspace as a means to further their cause, but the call is directed at defacing Web sites at worst. Significantly, there is no mention of using the Internet to achieve violence and destruction, although these people likely are planning such activities.

1. Defining Cyberterrorism

In the testimony to the Special Oversight Panel on Terrorism, [Denning2, 2000] defined cyberterrorism as:

> Cyberterrorism is the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives.

Denial of service attacks are clearly unlawful attack against computers, but it is not often known if the objectives are political or social. But Web sites sponsored by terrorist organizations are more apparently political and would therefore seem to conform to a cyberterrorist's tactics. This definition is also echoed by J.T. Caruso of the U.S. FBI, in his testimony before House Subcommittee on National Security, Veterans Affairs and International Relations on March 21, 2002:

> Cyberterrorism – meaning the use of cybertools to shut down critical national infrastructures (such as energy, transportation or government operations) for the purpose of coercing or intimidating a government or civilian population.

Many examples of cyberterrorism in the media seem to be derived from the definitions above. A 2001 Business World report listed as examples of cyberterrorism [Yam, 2001]:

- defacement of U.S. Web sites after the April 1, 2001 collision between a Chinese jet fighter and a U.S. surveillance plane;
- theft of information from the U.S. Department of Defense computers regarding U.S. troop movements, by Dutch hackers during the 1990-91 Persian Gulf War (the hackers tried to sell the information to the Iraqis but the Iraqis thought it was a hoax);
- penetration of computers at a U.S. Air base in Guam by a 15-year old Croatian youth.

However these examples would not satisfy the follow-on to Denning's definition above:

> Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not.

With this qualification, it would seem that the many examples cited by the media have been misleading. Some have argued that there have been no acts of cyberterrorism to date precisely because of the above prerequisites. Interestingly, the National Strategy to Secure Cyberspace, a document released by the Bush Administration in February 2003 to provide a framework for the protection of the national Information Technology Infrastructure, makes no mention of cyberterrorism, cyberterror or cyberterrorists. Instead, more generic terms like cyber attacks and cyber threats are used. Likewise the Center of Strategic and International Studies chose to use the terms Tactical and Strategic

Information Warfare rather than cyberterrorism [CSIS, 1998]. For the purposes of unambiguity within this thesis, Denning's full definition will be adopted.

2. Cyberterrorist "Camps"

The different views on cyberterrorism can be broken down to fundamental issues. We see disagreements about basic definitions of cyberterrorism, the threats that it poses, its utility to the terrorists, and its effects if played out. Any of these will lead to a different perspective on cyberterrorism. For the purposes of description and analysis they have been split into different "camps".

The first camp belongs to the "death-knell" who warn that it is only a matter of time before a cyberterrorist attack happens. Since most countries and other non-state adversaries know that they cannot match the US in the conventional military realm, cyber warfare is an increasingly viable alternative. This is accentuated by the growing reality that in many countries, their most valuable assets are in electronic storage and not their treasuries. With the information revolution, it has become easier to obtain the technical wherewithal to conduct IW activities using widely available commercial software and hardware. In addition, the Internet has provided a convenient and wide-reaching means for hacktivism – a fusion of hacking and activism – and other hacker activities. Each year, there are tens of thousands of computer attacks against the Pentagon. IW specialists estimate that with a budget of no more than $10 million, a well prepared and coordinated attack by fewer than 30 computer hackers strategically located around the world could "bring the United States to its knees", shutting down everything from power grids to air traffic control centers to emergency services. The basis for this assessment was probably made from the experience drawn from Exercise ELIGIBLE RECEIVER in 1997, in which a Red Team pretending to be North Korea was formed to carry out computer attacks against various government sites using hacking tools freely available from some 1900 Web sites on the Internet. Not only did they succeed in bringing down many key command-and-control systems, only 4 percent of those targeted were aware they were being attacked, and of these just 1 in 150 reported the intrusions to their superiors [CSIS, 1998]. The recent Slammer worm stopped Internet trading

activities of the South Korean stock exchange [Tullett, 2003]. Had a similar worm been planted by the North Korean military to subvert the South Korean defenses prior to a hypothetical invasion, the results could have been devastating for the South. Paradoxically, the goal of the "death-knell" camp is to ensure that its prophecies are never realized; actions taken as a result of the warnings should deny or at least reduce the probability of success for cyberterrorists.

The second camp comprises the "improbable" who believe that terrorists are more interested in physical violence and do not have the wherewithal to carry out sophisticated cyber attacks. So long as physical violence and destruction continue to draw publicity, fear and the appropriate public responses that feed their cause, there is little reason for a change of methods. A 1999 NPS study on the prospects and implications of cyberterror found that the ability of a terrorist group to carry out cyberterrorist attacks depended on firstly, the group's predilections toward cyberterror, and secondly, its means to do so [NPS, 1999]. The first requirement is not a given, since there are groups that prefer to stick to the more traditional means of physical destruction and violence. The second requirement implies a steep information technology learning curve that would take several years of effort for those groups that choose to develop an internal capability before any attacks can be effectively made. The combination of these two requirements significantly narrows the probability of cyber attacks by many terror groups. Some within the "improbable" camp think that the Internet is more likely to be used as a tool for cyberplanning than for out-and-out cyberterrorism [Thomas, 2003].

Thirdly there is the "nothing new" camp who claim that cyberterrorism is plain old terrorism executed in a different realm. Those in this camp distinguish it by calling it *technology-enabled terrorism* [Lang, 2002] or *information terrorism* [Devost et al, 1996]. While there is no doubt that the threats posed by technology-enabled terrorism are real, the contention is that they are no different from the more well-known forms of terrorism. In the case of technology-enabled terrorism, however, protection must be commensurate with the nature of the threat. Thus, network security measures, intrusion detection systems, encryption

and the like against electronic and network attacks are in order. One argument against cyberterrorism being merely terrorism in a different guise is whether cyberspace introduces new threats where there were none. A frequently cited example is SOLAR SUNRISE: in February 1998, two teenagers from California and one from Israel disrupted possible troop deployments to the Gulf when they launched attacks against the Pentagon's systems, NSA, and a nuclear weapons research lab using a well-known operating system vulnerability [CSIS, 1998; Denning1, 1999]. While these three teenagers did not have terrorist intent, the means and potential damage that could have been caused are no different from what a cyberterrorist might attempt.

The "cry wolf" camp assert that threats have been exaggerated since there have been no known acts of cyberterrorism to date, and certainly none of the scale that was seen on September 11, 2001. The Symantec Internet Security Threat Report covering January to June 2003 covered details of malicious code, Win32 viruses, the Slammer and Blaster Worms, spam activity, but made no mention of cyberterrorism or even terrorist-related cyber activities [Symantec, 2003]. Indeed, some have argued that the hype surrounding cyberterrorism is perpetuated by vendors for commercial gains. In addition, the more common forms of cyberspace attacks, such as Web site defacement, denial-of-service attacks, Internet fraud, and scams, do not kill people or destroy property the way terrorist attacks do [Love, 2003].

Finally, there is the "realist" camp who advocate that the real cyber threats are not from terrorists but criminals who commit cybercrimes. This thinking is borne from statistical evidence which show that most of the illegal activities stem from scams, frauds, identity theft, credit card theft, as well as hackers who are not in it for the money. In November 2003, the London Financial Times reported that hackers were exploiting computer vulnerabilities to carry out cyber extortion against online businesses. By carrying out distributed denial-of-service (DDoS) attacks, they were able to bring down the sites of their targets and threatened more attacks unless the businesses paid up. The reality is that the rate at which new Web sites are created – more than one every four seconds – makes the job

of law enforcement in cyberspace difficult. This is aggravated by the fact that the retention of computer talent in government agencies is constantly being threatened by the monetary lure of the private sector [CSIS, 1998].

While it is clear that there are different views on the threat posed by cyberterrorism, they all tend to agree that some form of threat exists, even if they disagree in its degree. They also agree that the targets are rife and attractive. Perhaps the question that needs to be answered is not what is the degree of the threat, but what has been or needs to be done to mitigate, address, counter, combat the threat.

C. THE CYBERTERRORISM THREAT

1. Motivations

In the section on terrorism, we saw that the main motivations for terrorism were political, ideological or religious. If cyberterrorism were truly a convergence of terrorism and cyberspace, then the same motivations would apply for cyberterrorism, albeit in a different medium. Many of the Web sites set up by terrorist groups serve the objectives of politics, ideology or religion.

Indeed, cyberspace provides certain advantages over a physical medium. For a start, it offers to cyberterrorism the benefit of remote and anonymous operations. It also avoids the need for handling physical weapons and explosives, and the attendant risk of spectacular failure of botched attempts when bombs explode prematurely. Cyberterrorist attacks are also likely to reap as much publicity as physical attacks [Denning2, 2000]. Additionally, cyberspace has enabled small players to create massive disruption, as for example through the creation and release of the ILOVEYOU and Nimda viruses or the more recent Blaster worm. This means that terrorists groups can get onto the world stage and create disruption and destruction on a scale that belies their size [CSIS, 2001].

Cyberspace attacks are not without disadvantages. Those viral or worm attacks that have had great reach were the result of the attacks going out of control; it may be difficult for cyberterrorists to control their attacks to inflict the

desired level of damage. Cyber attacks are probably less responsive to the whims of the terrorist leaders than physical attacks due to the lead time required to study the networks and gain access. Finally, as pointed out by the "improbable" camp above, a strong counter-motivation would be the effectiveness of tried and tested methods. It may still be easier to destroy a building with a car bomb than to take out all its computers with denial-of-service or worm attacks. This could well be the reason why little has been happening in comparison at the cyberterrorist front.

2. Actors

The existence of different cyberterrorist "camps" and forms of cyber attacks suggests that there may be more than just one type of cyberterrorist. Moreover, the nature of the medium enables cyberterrorists to be quite different from typical terrorists. Here we examine four possible categories of cyberterrorists and assess their threat.

Many of the well-known viruses such as the Morris worm, the ILOVEYOU virus, and the Chernobyl virus that have plagued cyberspace were the work of individuals. Recent history has also seen the likes of individuals who have created widespread damage, fear, and psychological trauma among the population, such as Ted Kaczynski (The Unabomber), Tim McVeigh (Oklahoma City Bomber) and John Muhammed (Washington D.C. sniper). Put the two types of individuals together and we get lone cyberterrorists. Many virus writers do so for the adventure and intellectual challenge, not for the sake of creating havoc [Denning1, 1999]. Moreover, the damage created by viruses and worms tend to be economic in nature, and have not cost human lives. As such, a lone cyberterrorist is more likely to be a Kaczynski or McVeigh with relevant computer skills, rather than a hacker or virus writer intent on killing others. Given a lack of precedents, the threat of a lone cyberterrorist appears to be low, but not improbable.

A small group of technically-skilled extremists could combine their abilities to create a well coordinated cyberterrorist operation. The Japanese Aum Shinryko cult were so well-developed in their software capabilities that they acted

as the software subcontractors to companies that were awarded contracts by the Japanese government. By the time the link was discovered in March 2000, the cult had already been receiving classified tracking data on Japanese police vehicles [Denning2, 2000]. Such groups may be considered to be a greater cyberterrorist threat than lone cyberterrorists because they have proven their ability to carry out such acts. In the case of the Aum Shinryko cult, they had already been found guilty of the Tokyo subway attack that killed 12 and injured 6000 others. Now their software abilities suggest that it would not take much for them to translate their violent goals to the next level in cyberspace.

Large religious terrorist organizations such as Al Qaeda with a track record in physical violence are another category that may embark on the cyberterrorism route. As it is, most of them have a presence in cyberspace and have even advocated electronic Jihad. [Ashley, 2003] measured the Al Qaeda cyber threat against the Defense Intelligence Agency threat-analysis methodology based on the existence, capability, intentions, history, and targeting of the threat and concluded that Al Qaeda posed a critical cyber threat to the U.S. However, a potential shortcoming in this assessment is that Al Qaeda does not have a proven cyber capability, notwithstanding that Osama bin Laden had boasted of the existence of “Muslim scientists” among his strike force. While it may only be a matter of time before they strike, the cyber threat currently posed by Al Qaeda and similar groups may not be any more imminent compared to the previous category. Judging from the number of recent bombings attributed to such religious fundamentalist groups, and the technologically unsophisticated nature of the bombings, it would seem that they continue to favor the traditional methods.

The final category belongs to information-warfare groups that are sponsored or backed by hostile governments. There are at least two levels of information-warfare groups, each with differing capabilities and origins. At the official level there are cyberwarfare units formed by governments to attack enemy information systems, as well as to protect their own. A report on the military power of the People’s Republic of China [IWS, 2003] cited the presence

of “Special information warfare units [that] could attack and disrupt enemy C4I, while vigorously defending PRC systems.” Strictly speaking they are not cyberterrorist outfits, but the scale and degree of harm that they were created to inflict are similar. These government units are restrained in peacetime by international treaties and therefore cannot openly carry out vulnerability scans of an adversary’s systems, for example. The same report also hints at the presence of Nationalistic hackers who form an unofficial organizational level. These are self-declared patriots who take it upon themselves to attack the information systems of other countries when they are in conflict. But the Chinese are not alone. [Dunnigan, 2002] reports widespread hacking by Russians, Taiwanese, Israelis, Indians, Pakistanis and Americans following international incidents such as those mentioned in the previous section. Many of these hackers contravene their own national laws when they carry out such activities, but often they are left alone by their governments so long as their activities fall in line with “national interests.” [Devost, 1995] suggested the employment of hackers as a national resource because they have the requisite skills for attacking an adversary’s information systems. Some evidence exists to suggest the presence of a third level sitting between the first two. In 2001, Taiwan allegedly unleashed several viruses against China but the viruses spread around the world. Taiwan has not admitted to these incidents [Dunnigan, 2002], but the scale and targets of the apparently anonymous attacks suggest that clandestine groups are operating with covert government links. This middle clandestine level appears to pose the most significant threat because they have many of the resources of the official groups and the freedom of action of the outlaw hackers.

3. Targets

In the Second World War, strategic bombing targeted the weak belly of the adversary, focusing on population and industrial centers in an effort to demoralize the frontline troops and undermine their war-making machinery. The information technology revolution and improved military technology have made possible precision bombing and targeting, thereby reducing significantly the killing of innocent civilians and the associated political backlash. However, the

information technology revolution has also shifted the balance of power to the commercial sector, as far as innovation, development, resources and the state-of-the-art are concerned. Thus it would seem that in the age of cyber warfare, attackers are now drawn towards those who rely heavily on information technology, or who would have much to lose by being denied it. In this case, the commercial sector would be as lucrative a target as the government. The frontline in cyber warfare has shifted back to the population and new industrial centers of information technology.

Computers, computer servers and computer networks are usually considered the *targets* of cyber attacks. As the October 2002 attack on the nine core Internet domain name servers showed, such attacks have indeed taken place and this scenario is therefore not unthinkable. In these denial-of-service (DoS) attacks, target computer servers are flooded with more messages than they can effectively handle, thus denying service to genuine users. In some cases such as distributed denial-of-service attacks, the flooding is from the accumulation of messages from many other "zombie" servers on which malicious programs had been secretly planted to make them collaborators in an illegal activity unbeknownst to them. One of the most spectacular attacks occurred between 7-9 February 2000 when a massive attack crippled popular Web sites like Yahoo.com, Amazon.com, CNN.com, ETrade, and EBay. During that period, it was estimated that average surfing times were delayed by 26 percent on average, due to the additional traffic on the Internet as result of the attacks [Dunnigan, 2002]. These zombie servers could be considered both as targets and weapons of the cyber attack, as they first needed to be targeted for "conversion" before they became part of the attackers' arsenal.

Many cyberterrorism scenarios involve disabling the Internet or at least disrupting a significant portion of it. Notwithstanding that it will involve massive amounts of resources, coordination and know-how, disabling the Internet would surely cripple the communications means by which many organizations and agencies do their business and is therefore a high-payoff target. However, cyberterrorists who seek to disable the Internet must surely know that it would

also disable their means to carry out further cyber attacks. So such scenarios should perhaps be refined to paint the Internet as the last thing to go down, not the first.

The cyberterrorism threat is not easily detected or anticipated. At best it can be deterred; at worst the system will have to absorb the first blow and recover quickly. Some scenarios suggest retaliation, but it is often difficult to determine the attacker and there may be associated legal issues.

4. Understanding the Threat

The gravity of the cyberterrorism threat may be measured from two parts: the vulnerability of targets which if exploited could lead to violence, physical destruction or death, and the ability and motivation of terrorists to carry out such attacks [Denning2, 2000; NPS, 1999]. There are many scenarios in which attacked information infrastructures can lead to destruction and death. For example if the computer systems of an air traffic control system (ATCS) are hacked into and manipulated, it could result in a collision of aircraft in mid-air. Following FBI reports of Al Qaeda members researching information on the Supervisory Control and Data Acquisition (SCADA) infrastructure which manages U.S. water and wastewater systems, new scenarios emerged with terrorists taking remote control of such systems and releasing dammed water onto civilian populations downriver [Ashley, 2003]. Other scenarios feature a blending of cyber attacks with physical ones (bombs or attacks on critical infrastructure). For example, a large or “dirty” bomb could be detonated in a crowded marketplace with the ability of emergency teams to respond hindered by a power and telecommunications failure caused by the cyberterrorist wing of the terrorist group. ELIGIBLE RECEIVER and SOLAR SUNRISE have shown that certain critical infrastructures could be susceptible to such incidents.

The second part of cyber threat assessment deals with the ability of terrorist groups to carry out cyber attacks. Of the four types of actors mentioned, the first three have a proven propensity for wanton and indiscriminate violence. That this has not occurred in cyberspace suggests that they either lack the means or will to do so. However, this state of affairs cannot be relied upon as the

terrorist ranks are gradually filled with newer and younger recruits who have grown up with information technology. A more sinister threat of cyberterrorism is when cyber attacks carried out by any of the actors remained undetected. Those attackers that are discovered either lack sophistication or are too disorganized to conduct any coordinated attack. The more serious threats are likely unseen, complex and distributed. Attackers could conduct covert reconnaissance for years to ascertain critical information assets before execution of actual operations [CSIS, 1998]. Some have called this the new terrorism [Gordon & Ford, 2002]. In this scenario, Web site defacements, hacktivism and hacking intrusions are probably only the tip of the iceberg.

5. Combating the Threat

As [Betts, 2001] concluded on whether there will be another catastrophic Intelligence failure like September 11, it is a question of *when*, not *if*. So it is just as important to prepare to manage the damage as it is to prevent it. The Defense Science Board suggests that "deterrence in the information age is measured more in the resilience of the infrastructure than in a retaliatory capability" [CSIS, 1998].

Cyberterrorism needs to be fought with the same breadth of measures and intensity accorded to terrorism. Hence there is a need for an appropriate framework for law enforcement and intelligence gathering to thwart the efforts of cyberterrorists. In the U.S., initiatives include the PDD 63 (President Decision Directive), the establishment of the NIPC (National Infrastructure Protection Center), the ISACs (Information Sharing and Analysis Centers) for the private sector owners of critical infrastructures, and Infragard, a community of professionals with an interest in protecting their information systems [Rodgers, 2003; CSIS, 2001]. This year, the Bush Administration released the National Strategy to Secure Cyberspace document to consolidate the U.S. government's commitment to fight cyberterrorism and other cyber threats. Singapore has recently enacted a cyber law akin to the American Patriot Act that would enable the authorities to initiate pre-emptive action against hackers in Singapore and seek Interpol's assistance for hackers overseas [STI, 2003]. The enactment of

such laws is not without objections. There are outcries by the libertarian groups who feel that such powers are too

wide-ranging and can lead to a significant loss of electronic privacy. They also question the availability of checks and balances to ensure restraint and prevent abuse by the authorities.

Other methods of combating cyberterrorists involve the use of honeypots and software decoys. The former collects data to better understand the techniques employed by computer intruders, while the latter seeks to provide additional layers of protection against them. Both of these will be covered in more detail in subsequent chapters.

III. DECEPTION

> In 149 BC, the famous strategist Kong Ming of Shu, launched an attack against the state of Wei by sending an advance force to scout for the enemy. Leading the army of Wei was Suma-I who also sent an advance force of fifty thousand troops. The two vanguards met and engaged in battle but the Wei forces were superior and won the day. The defeated Shu vanguard raced back to the main body of Kong Ming's army whose troops, seeing the look of fear in the faces of their comrades, thought that the enemy was upon them and fled in panic. Kong Ming and a few bodyguards fled to the city of Yangping with the Wei army in hot pursuit. Vastly outnumbered and unable to either retreat or sustain a siege, Kong Ming played a last resort strategy that made him famous throughout China. He removed all the guards and battle flags from the walls and had all four of the city gates flung open. When Suma-I approached the city he could see only a few old men nonchalantly sweeping the grounds within the gates. Kong-Ming was seen sitting in one of the towers smiling and playing his lute. Suma-I remarked to his advisors: “That man seems to be too happy for my comfort. Doubtless he has some deep laid scheme in mind to bring us all to disaster.” As they stood spell bound, the strains of Kong Ming's lute reached their ears and this only heightened their sense of foreboding. Such peculiar behavior was too suspicious and, fearing a clever trap, Suma-I turned his army back and retreated. After the army left Kong Ming and his remaining troops departed in the opposite direction and made their way safely back to their capital. [Verstappen, 2003]

A. THE MANY FACES OF DECEPTION – DECEPTION IN ACTION

1. Deceptions in Nature

The master practitioners of deception are to be found in nature, since it often is a matter of life or death. The puffer fish transforms itself into an enlarged ball shape thus giving the impression that it is more than a mouthful to its predators; the buff-tip moth’s woody shape and colors makes it look more like a broken twig to escape the attention of predatory birds; the hawk moth caterpillar inflates the front of its body to look like a snake’s head when confronted with a threat; the tasty viceroy butterfly mimics the wing pattern and color of the bitter-tasting monarch butterfly. Also, the monkey-slug caterpillar grows hairy fake legs

that break off harmlessly when bitten by a predator; and the European grass snake attempts to deter a predator by puffing itself to look bigger and hissing loudly, then plays dead by rolling belly up and hanging its tongue out. [Krautwurst, 2001].

For these and many other animals, deception is a natural and important tactic that could help determine the survival or extinction of their species. [Gerwehr & Russell, 2000] proposed several principles of deception based on animal biology and behavior. They found that species of all types, including plants, use many different types of deception in all kinds of life-supporting environments. Deception is also used by both predators and prey. Even minor applications can confer selective advantages.

2. Deceptions in Human History

> All warfare is based on deception.
>
> − *Sun Zi Bing Fa*
> (Sun Tzu: *The Art of War*)

Human history abounds with stories, anecdotes and legends of deception, the most notable of which are in military history. One of the most famous historical proponents of deception is the ancient Chinese military philosopher Sun Zi, whose writings in the 4th Century B.C. clearly advocated the use of guile and deception in trying to overcome one's enemy. The opening story of this chapter is but one of the many examples of deception to emerge from the Far East, where Sun Zi's writings had had a great influence [Whaley, 1980].

The most well-known ruse in military folklore is probably the Trojan Horse in which the Greeks devised a large wooden horse in 1183 B.C. as a means to sneak thirty warriors hidden in its belly past the city gates of Troy. The Trojans, believing that the Greeks had finally given up after ten years of siege, took the horse into the city as a victory trophy. While the Trojans celebrated the night away, the thirty Greek warriors emerged from the horse and threw open the city

gates for the rest of the Greek forces, which were lying in wait beyond the horizon, to conquer the city [Bell & Whaley, 1991].

Deception is not uncommon even in the Bible: In Genesis Chapter 27, Jacob obtained his father Isaac's blessings by fraud. As Isaac was old and almost blind, Jacob was able to pretend to be his brother Esau by wearing his brother's clothes and made himself hirsute like his brother by covering his arms and the smooth part of his neck with the skins of kids. In doing so he deceived his father's sense of smell and touch respectively. In Joshua Chapter 8, Joshua devised a stratagem to lure the King and people of Ai away from their city. After positioning some thirty thousand troops in a concealed location to the rear of the town, Joshua led the rest of his forces in an advance on the town. As Ai's troops came out to engage the enemy, Joshua and his troops bid a hasty retreat, giving the impression that they were in disarray. Sensing an opportunity, the King of Ai led his troops in pursuit of the falling enemy. Meanwhile, the troops that were concealed by Joshua ran out of their ambush to capture the undefended Ai.

The last century saw the introduction of new weapons and technology hitherto unknown in warfare. All the same, these new capabilities gave rise to new methods of deception, but with the same effect – misperception and surprise. During the Second World War, the Allied Forces conceived a series of ambitious and elaborate deception plans code-named BODYGUARD in an attempt to conceal the Allies' plans for the invasion of Normandy. The intent of BODYGUARD was firstly to deceive Hitler into dispersing his troops throughout Europe so that the Germans did not have sufficient strength at Normandy to repel the landings there; secondly to delay German response to the actual invasion by confusing their Signal Intelligence and administrative-support systems. The deceptions were so successful that two weeks after the landings, Hitler was still under the impression that the activities at Normandy were a feint. Instead of reinforcing the defenses there, he stubbornly maintained his troops at Pas de Calais where he thought the main landings would take place. In the battle for the liberation of Kuwait in 1991, the Coalition Forces staged several demonstrations by the Navy and Marines to suggest to the occupying Iraqis that

the main Coalition attack would come from the Saudi-Kuwaiti border and from the sea, thereby fixing the Iraqi divisions to the defense of Kuwait's southern border. The demonstrations included the positioning of a large amphibious task force, together with air refueling and various training activities in the Persian Gulf off Kuwait. These activities were further reinforced by the absence of air attacks at the Western front where the main attacks were going to take place. Operations conducted by Special Forces added to the Iraqi confusion on the source of the main attacks [Joint, 1996].

B. DEFINING DECEPTION

In one definition, deception is simply the "distortion of perceived reality" [Whaley, 1982]. But as seen in the previous paragraphs, there are many faces to deception, which makes an overarching definition difficult. Note how the following definitions derive from their different perspectives:

> The military perspective [Joint, 1996] – military deception is defined as being those actions executed to deliberately mislead adversary decision makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions that will contribute to the accomplishment of the friendly mission.
>
> The Intelligence perspective [Shulsky & Schmitt, 2002] – deception is the attempt to mislead an adversary's intelligence analysis concerning the political, military, or economic situation he faces, with the result that, having formed a false picture of the situation, he is led to act in a way that advances one's interests rather than his own.
>
> The theoretical perspective [Whaley, 1982] – deception is information designed to manipulate the behavior of others by inducing them to accept a false or distorted presentation of their environment – physical, social or political.
>
> The "historical" perspective [Carr, 2000], from *Sun Zi Bing Fa* – when able, seem to be unable; when ready, seem unready; when nearby, seem far away; and when far away, seem near. If the enemy seeks some advantage, entice him with it… If he is strong,

> evade him. If he is incensed, provoke him… Attack where he is not prepared; go by way of places where it would never occur to him you would go.

A common characteristic among these definitions is the notion of misperception. This will be elaborated further in the next section.

1. Taxonomy of Perception

[Whaley, 1982] developed a general theory of deception on the basis that deception is a matter of misperception. For this, he proposed a taxonomy of perception, as shown in Figure 1, to show the relationships between perception, misperception and deception.

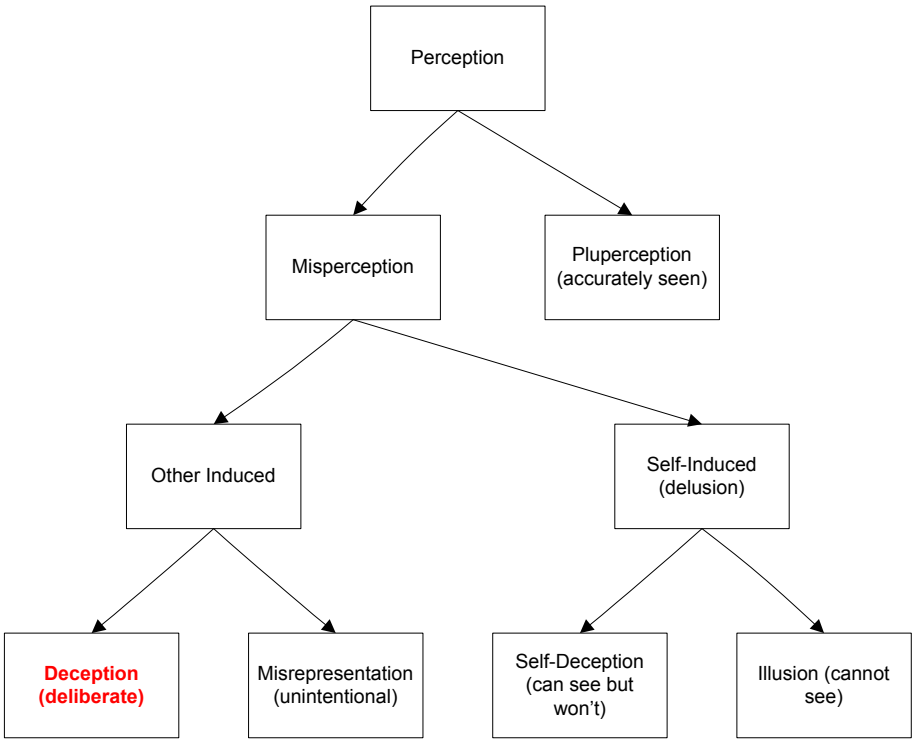

Figure 1. A Taxonomy of Perception (After [Whaley, 1982])

The taxonomy distinguishes between the other-induced and self-induced misperception, as well as between deliberate and non-deliberate acts. Self-induced acts are also known as delusion while non-deliberate or unintentional acts are considered misrepresentations. For deception to take place, the act

must be a deliberate one, with a specific intent and effort on the part of the deceiver, with the purpose of inducing a misperception by the victim.

2. Structure of Deception

A different structure of deception was also proposed by Whaley in [Whaley, 1982] as comprising simulation (showing the false) and dissimulation (hiding the real).

The Structure of Deception			
Dissimulation (Hiding the Real)		**Simulation** (Showing the False)	
Masking (to eliminate an old pattern or blend it with a background pattern)	• Concealing one's own characteristics • Matches another's characteristics	**Mimicking** (to recreate an old pattern, imitating it)	• Copies another's characteristics
Repackaging (to modify an old pattern by matching another)	• Adds new characteristics • Subtracts old characteristics	**Inventing** (to create a new pattern)	• Creates new characteristics
Dazzling (to blur an old pattern, reducing its certainty)	• Obscures old characteristics • Adds alternative characteristics	**Decoying** (to give an additional, alternative pattern, increasing its certainty)	• Creates alternative characteristics

Table 1. The Structure of Deception (After [Whaley, 1982]).

Table 1 can be interpreted in several ways. First, it provides a breakdown of the two main forms of deception, dissimulation and simulation. Secondly, it shows the dependency relationship between the two: for deception to occur, simulation cannot exist without dissimulation, because all deception involves hiding [Bell & Whaley, 1991]. Moreover, the two main forms are often present together in an act of deception. When something is hidden, something else can be shown either in its place or elsewhere, thereby inducing the false perceptions about what is happening. This duality also applies to the subcategories. Masking is present with mimicking, repackaging with inventing, and so on, as shown by the horizontal color shadings. Finally, the level of effectiveness of deception decreases as one goes down the table.

C. THE VALUE OF DECEPTION

Even with modern technology, deception is valuable. This is because deception can act as a force multiplier that offers advantages to either the attacker or defender, whether they are strong or weak.

1. For the Attacker

Deception can enable an attacker to achieve their objectives more easily. The 1991 Persian Gulf War was an instance of a strong attacker (the U.S. led coalition forces) against a weak defender (Saddam Hussein's Iraqi Forces). By fooling the Iraqis into believing that the attack would come from the south and east, the main attack which came from the west was able to proceed with great speed.

An attack by a weak force is not a typical occurrence in conventional warfare, but in the history of deception this is not uncommon. One example in the Bible is Gideon's creation of a dummy force to deceive his enemies [Bell & Whaley, 1991]. Technological surprise can also help as evidenced by the famed slingshot used by David against Goliath.

2. For the Defender

Deception may enable a weak defender to achieve victory without force. The story of Kong Ming at the opening of this chapter is one classic instance. Deception can also be regarded as a worthy and humane alternative to violent conflict. Tactics such as bribing the mercenary officers of the enemy, circulating false reports to degrade enemy morale (or boost their own) or fabricating treasonable letters to frame enemy commanders enabled the Byzantine empire to survive almost a thousand years against the myriad forces that surrounded them [Dunnigan & Nofi, 1995]. A strong defender can also benefit from the use of deception to take the initiative away from the attacker. Deception could entice the attacker to commit his forces at a time and place to the defender's advantage. In early 1944 the British started a massive bombing campaign against reinforced V1 and V2 missile launchers in Pas de Calais, France. The campaign was successful, rendering the sites unusable and the surrounding roads impassable to heavy equipment. Although the Germans switched the missile sites to mobile

ones for the V2 and easily erectable ones for the V1, Hitler ordered that repair work be started on the fixed sites even though there was little hope of ever using them. This forced the British to continue to focus their attention and precious bomber resources on the fixed sites. The catch was that had the British seen through the deception, they might have disregarded the sites and allowed the repair work to continue until the sites were actually usable once again [Jones, 1989]. This was an instance of a feint that served its purpose whether or not it was detected as such.

3. Nesting Deceptions

Deceptions that are detected could hide a second deception as a form of nested deception where one deception is used to hide another. In the Second World War, the British commander Brigadier Dudley Clark created A-Force that employed a host of trickery in the North African desert, such as tanks that looked like lorries and vice versa, and lorries that carried devices to create tank tracks in the desert sand. In the battle of El Alamein against Rommel in 1942, Brigadier Clark's A-Force created a string of dummy guns enmassed on the southern front of the battle area. However, these were detected as such by the German Afrika Korps early in the battle, and were consequently disregarded by the Germans. But the dummies were replaced thereafter by real guns which were used to support a subsequent attack [Jones, 1989].

It is also a common belief that a ruse once used should not be repeated, but history is replete with recycled tricks [Whaley, 1987]. In 1864, General Sherman marched 180 miles through the eastern Confederacy toward Atlanta along a single railway line. Throughout his drive, he was aware that the Confederates knew his logistic tail was confined to that single line, and yet he was able to repeatedly surprise his enemies as to the time and place of his attacks by choosing either the left or right flank of the railway line to attack and defeat them [Bell & Whaley, 1991].

D. THE DECEPTION PLANNING PROCESS

Successful deception starts with a deception plan. [Gerwehr & Russell, 2000] describe their three-stage deception process as one in which “the ends dictate the means.” This is reinforced in [Cohen, 2002] who observed that deception plans are driven by the desired effect on the target. [Fowler & Nesbitt, 1995] proposed six fundamental rules to guide a deception planner towards success. The U.S. Joint Doctrine for Military Deception [Joint, 1996] contains a six-step deception planning process that requires command involvement and approval at each stage of the process. [Whaley, 1982] has suggested a ten-part step-by-step planning process for deception to increase the probability of success as follows:

1. Identify the strategic goal
2. Decide how the target should react
3. Determine what the target should perceive
4. Decide what to hide and show
5. Analyze the pattern for hiding
6. Analyze the pattern for showing
7. Design the desired effect with the hidden method
8. Sell the effect to those who are executing the deception
9. Decide the communications channels to transmit the deception
10. The target buys the effect and falls for the deception

In addition to these ten steps, the deception planner must prepare for contingencies in the event that the deception fails. During the course of the deception, the planner also seeks feedback to ensure that the target is responding in the expected way.

E. DECEPTION, INTELLIGENCE AND COUNTER-DECEPTION

Deception and intelligence failure are closely intertwined because a successful deception by one side is usually the result of an intelligence failure by the other [Shulsky & Schmitt, 2002]. The Second World War deception operation BODYGUARD was successful because German intelligence failed to detect the Allies' true intentions. Correspondingly, any deception effort must ensure that the sensors in the enemy's intelligence collection layout are present and capable of recognizing the intended ploy ("buying the effect") while our own intelligence collection assets must be deployed to provide feedback on our deception effort. This is reiterated in the Joint Doctrine for Military Deception [Joint, 1996] which stipulates that intelligence and counter-intelligence are critical for identifying the enemy's decision makers, ascertaining their perceptions and information gathering capabilities, as well as assessing reaction to the deception operation.

Deception is also tightly linked with counter-deception, which refers to the detection of deception [Whaley, 1982]. Since it is not possible to hide or show an object or event to the "full extent", incongruities can occur in every deception operation. An intelligence analyst need only detect one inconsistency among the collected data to sense that something is amiss in the analysis. A cheat's first mistake is probably his last. [Jones, 1989] wrote in 1942 that "No imitation can be perfect without being the real thing." While it is always possible to detect a deception in theory, detecting a deception can usually be very difficult. This is even more so when it concerns strategic deception, as the counter-deception analyst is dealing with intentions or motives at the highest levels [Kam, 1988]. Even when incongruities are spotted, it is usually easier to believe that a mistake or omission has been made. When the British Secret Service MI6's Dutch agents sent encrypted messages back to headquarters in 1941, they were required to include a security check to prove that the message was not spoofed or sent under coercion. Unfortunately, the staff officer in charge in London told a "Dutch agent" to follow proper procedure and instructed the agent on the use of the security check. The Germans who were impersonating the "Dutch agent" were

now unwittingly informed about it. This enabled the Germans to continue their *Nordpol* deception operation against the British up until 1944 [Shulsky & Schmitt, 2002].

Understanding deception itself is a first step towards counter-deception. A renowned British practitioner of deception in the Second World War, Dr. R. V. Jones, who was an intelligence officer, established two principles for unmasking deception [Jones, 1989]:

> (1) in any channel of intelligence through which you may be deceived, arrange to work down to a greater level of sophistication than your opponent has expected you to adopt, and (2) bring all other possible channels of intelligence to bear on the problem, to see whether the evidence that they can provide is consistent with the evidence in the channel through which you suspect you are being deceived.

It is also possible to employ deception to acquire intelligence. Scouts reconnoitering for the enemy sometimes engage in a tactic called “recce by fire” to trick the enemy to return fire thereby revealing their positions. A variation of this is “fighting fire with fire” in which the adversary’s use of deception is defeated by our own use of deception. An example of this in nature is the boomslang snake’s use of its own camouflage to defeat the camouflage of the chameleon. When the unsuspecting chameleon forages about in the proximity of the snake, its movements reveal the lizard to the predatory snake.

F. PITFALLS OF DECEPTION

1. Traps That Backfire

A deception that is detected could be used against the deceiver. When General Navarre’s French garrison secured the mountain top at Dienbienphu in 1953, he saw it as an opportunity to lure General Vo Nguyen Giap’s Viet Minh troops towards his position of strength. But Dienbienphu became a symbol of French military prestige worldwide. This had the unfortunate consequence that Dienbienphu had to be held at all costs by the French, and a victory by General

Vo would have severe political repercussions for the French. The French were caught in their own trap as evacuation had also become impossible [Whaley, 1987].

2. Active and Passive Deception

Given the risks associated with deception, practitioners distinguish between passive and active deception. Passive deception such as camouflage and concealment is the safest and most easily enforced [Dunnigan & Nofi, 1995]. Most armies sport battle dress uniforms with disruptive pattern material and include camouflage and concealment in their field deployments and tactics. Aircraft and ships are also painted to enable them to break their silhouettes and better blend against their backgrounds. Special patterns may also be added. Stealth technology that is employed in new generation aircraft and ships strive to deceive electronic sensors.

Active deceptions can be risky because they are often unpredictable and complex to execute. The Joint Doctrine for Military Deception [Joint, 1996] stresses that "deception planners must carefully consider the risks involved versus the possible benefits of the deception." One risk of deception is that once detected by the enemy, the deception could be turned against the deceiver if the exposure is not known to the deceiver. A second risk pertains to the balance between secrecy and exposure: secrecy is needed to prevent dangerous leaks, but unaware friendly forces or allies could take action that could lead to unintended conflict, errors of judgment and fratricide. Many therefore conclude that the risks of active deception are so high that it would be better not to attempt it at all. Yet [Whaley, 1987] suggests that this is pessimistic advice.

3. Legalities

Another pitfall of deception involves the legality of deception. The Geneva Conventions state that the use of camouflage, decoys, mock operations and misinformation is permitted, but what is expressly prohibited is the use of perfidy. These are acts that, for example, gain the confidence of the enemy into believing that surrender would entitle them to protection under the rules of international law, when the real intention is to betray that confidence and annihilate them after

their surrender. But the reality is usually that the space between what is permitted and what is not is very grey. Creating decoy missile launchers to fool air surveillance is legal, but hiding the real missiles under a Red Cross banner, in a hospital building or a national monument is probably not. We could argue in this case that the deception is not ethical. Indeed, what is legal is not necessarily ethical. Hence deception is sometimes also justified by the outcome. That is, the means is justified by the ends when the cost of deceiving is higher than the cost of not deceiving. In the animal kingdom, the cost is clear – it is a matter of survival. In the human world, it could mean reducing loss of friendly lives if a deception operation was successfully carried out.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. CYBERTERRORISTS AND CYBER DECEPTION

A. DECEPTIONS IN CYBERSPACE

A new domain is being used today for human deception: cyberspace. Cyber deception has been especially successful because of the tendency of the average computer user to trust what they see on the screen to be authentic. A recent example of deception in cyberspace occurred in Oct 2003 when a fake FBI site sporting authentic FBI logos was discovered to be luring Internet users into divulging their bank account numbers [Sullivan, 2003]. In what is known as "phishing", an electronic mail was sent to users with a message seemingly from the FBI informing them about a massive theft of debit card numbers. A link was given to visit a supposed FBI Web site to key into a form their debit card numbers and account balance to check if their account had been compromised in the "theft". In actual fact, both the mail and the Web site were false fronts and instead of directing users to https://www.fbi.gov/debit_theft.html as it appeared, they were sent to a Web site hosted at fbi.x-web-x.com. The data entered into the fake FBI form would then be transmitted to a Russian electronic mail address.

Phishing is but one of the more recent manifestations of Internet fraud. The more common ones include phoney business opportunities, "official" or "government" information requests that demand information through questionnaires or forms, and investment fraud [Dunnigan, 2002]. The latter typically appears in the form of a sender (the crook) looking for an investment partner (the victim) to provide a bank account to which a large sum of money would be "transferred out" from a foreign account. Through the transaction the victim would be rewarded with a commission based on a percentage of that sum transferred. The enticement is that this commission usually runs into a large amount of money. Other variants involve an opportunity to join an investment promising high returns, or a lottery win that requires a bank account to which the prize money would be transferred. Whatever the style, the outcome of the enterprise is usually that the victim's bank account is cleaned out instead. The author himself has received (through a personal electronic mail account) several

of these electronic mails in the course of the past year alone, so the crooks are still hard at work in this day. Excerpts from some of these electronic mails are included below:

> … all I needed from you is to furnish me with your bank particulars:
> 1) Account name
> 2) Account number
> 3) Bank address, telephone and fax number
> For you to assist me transfer this money in your private bank account, the said amount is (Twenty seven Million Dollars) $27 Million. I am compensating you with 12% of the total money amount…

> … the family has asked me to seek for a foreign partner who can work with us as to move out the total sum of US$75,000,000.00 (seventy-five million United States dollars), presently in their possession …

> … I am hereby soliciting your assistance to provide a foreign bank account (Personal or company's) for the lodgment as acclaimed beneficiary since the over-invoiced contracts were dully executed by some foreign firms also. We have also mutually agreed to compensate you with 25% of the total sum …

> … For due processing and remittance of your prize to a designated account of your choice. Be categorically inform that any necessary obligation/requirement should be met by individual beneficiary towards remittance of your fund to your account …

Another form of deception in cyberspace involves social engineering, "getting people to do things they wouldn't ordinarily do for a stranger" [Mitnick, 2002]. Using a variety of techniques that prey on human goodwill, trust, helpfulness, gratitude, and gullibility, highly secure computer systems and networks can be compromised by attacking the weakest point, the human users. By pretending to be a new system administrator, technician or security consultant, social engineers can trick the victims into revealing passwords or remote-access numbers to enable them to break into computer systems. A further development in social engineering is the use of online translators and

relay telephony services that allow social engineers to exploit and overcome language barriers [Ollmann, 2003]. Relay telephony services are online services provided by telecommunications companies to help persons with hearing or speech disabilities through the use of an intermediary. This means that social engineer can conduct an anonymous attack on a victim who speaks a language that is unfamiliar to the social engineer without providing as many direct clues as to their deceptiveness.

Even in more mundane environments, the use of deception has also been an ongoing occurrence in information systems where multi-level security requires cover stories against unauthorized users, or in electronic commerce where some form of deception is employed in software agents that are used in price bargaining [de Rosis et al, 2004]. Other attack techniques that use deception include spoofing and masquerading, covert channel exploitation, false updates, man-in-the-middle attacks and software Trojan Horses. A software Trojan Horse is an “information warfare tool that is used to gain access to an information resource” [Denning1, 1999]. Examples of Trojan horses include logic bombs, additional instructions in memory and operating system modifications [Cohen1, 1998].

One interesting aspect in the use of cyber deception is whether computers can be deceived. Fooling a computer user is easy as the examples above have shown. The computer users are merely proving Whaley’s theory of perception [Whaley, 1982] that deception must take place in the mind of the person deceived. This same theory is challenged, however, when we consider whether a computer used in an attack, such as one based on an automated script, can be deceived since it does not have a “mind” that can be fooled. As it turns out, automated scripts are programmed with certain expected outcomes and these can be “tripped” when they encounter a surprise, or specifically, a deception. However, the question of whether more sophisticated attack software can be deceived by complex defensive deceptions is an open one. The answer may well be found amidst the ongoing competition between virus writers and anti-virus

software vendors, or between hackers and intrusion detection systems, where the opposing parties are constantly trying to outdo and outsmart each other.

B. THEORY OF CYBER DECEPTION

1. A Taxonomy of Cyber Deception

Others have sought to provide different perspectives based on context and other models. The taxonomy proposed by Dunnigan and Nofi [Dunnigan & Nofi, 1995] lends itself particularly well to understanding deception in cyberspace, as suggested by [Cohen2, 1998] and [Rowe & Rothstein, 2003]. Deceptions in cyberspace and cyber deception are used interchangeably here, and refer to the use of deception techniques in cyberspace, computers and computer systems. It should also be noted that this taxonomy is by no means definitive, but is meant to be illustrative.

a. Concealment

Concealment is hiding using natural means such as terrain and vegetation. Concealment is regarded as one of the oldest forms of deception and is still actively used in the animal kingdom. Cyberspace offers many options for hiding. A hacker can conceal malicious files or software in some obscure directory or in normal code within the target system, which are part of the system's "natural" environment. The newer versions of the Windows operating system use the NTFS file system which supports both a normal file stream as well as an alternate data stream. In Windows Explorer, the normal stream provides the expected contents of a file, while the alternate data stream enables an arbitrarily large amount of data to be hidden behind the normal file. This means that a hacker can hide files or programs behind other files in the target computer without the knowledge of the legitimate users [Skoudis, 2002]. Technology also allows for information hiding through techniques such as steganography where the very existence of the information being hidden is concealed. One example involves hiding messages within the noise of a digital image, in which some of the bits making up the image are used to encode a secret message without significantly altering the image [Denning1, 1999]. Those

who are aware of the existence of the message can proceed to decode it, and those who do not, remain ignorant.

b. Camouflage

Camouflage involves hiding with the use of artificial means, such as the use of cut branches and plucked leaves on oneself to better blend in with a forest. The proverbial wolf in sheep's clothing is another example of camouflage. In information systems, malicious software such as a logic bomb could be camouflaged by an innocuous filename. An example was demonstrated by [Anderson, 2002] in which a few lines of code were able to create a significant vulnerability in the target system, camouflaged as a corrupted packet within a Network File Server. Since corrupted packets are a common occurrence in networks, it was near impossible for intrusion detection systems or firewalls to single out the malicious one. Another form of camouflage is the use of "Easter eggs", in which "amusing tidbits" are hidden by creators in their products. The Web site www.eeggs.com is an archive of various Easter eggs, of which one of the more well-known ones is the flight simulator hidden within Microsoft Excel 97.

c. False and Planted Information

This refers to the feeding or planting of information that would cause the enemy to respond or react in a manner contrary to his own good. For such a technique to be effective, it is necessary to understand the behavior of the target and the ongoing context in which the deception is to be carried out. False information planted in computer systems could potentially divert or confuse attackers. For example, false instructions could be planted in hacker discussion forums or bulletin boards that describe how certain flaws could be exploited [Rowe & Rothstein, 2003]. However, such actions are probably not very beneficial for a cyber defense system since the hackers may not take the bait. Those who do may quickly find that the instructions are inaccurate and not pursue the attack. The detection of false information in computer systems is not necessarily difficult; a knowledgeable hacker is likely to recognize a honeypot. This technique is also difficult to execute because one can never be sure if the enemy sees the information at all as well as falling for it.

The Internet can be used to spread disinformation, rumors and false reports. A constant campaign of disinformation reinforced with images of Osama bin Laden manipulated to look healthy and happy could seriously undermine the global anti-terrorist efforts [Thomas, 2003].

d. Ruse

This is the use of tricks to make the enemy think that you are friendly when in fact you are not, such as using enemy equipment or wearing enemy uniforms. Network site (IP) spoofing is a common ruse to make the target network accept the attacker as friendly. With this, the attacker can convincingly forge certain kinds of electronic mail. For instance, the W32.Mimail.C@mm is a mass-mailing worm for denial-of-service attacks against hard-coded sites. It is distributed as a .zip archive which may include a file named photos.jpg.exe, giving the impression that double-clicking the file would open photos [Symantec, 2003]. Ruses are not very useful as a defensive technique, partly because it invites legal complications, and partly because it is difficult to pretend to be a hacker.

e. Display

A display attempts to make the enemy think that something is there when there is none. An old example is the tying of branches to horses and making them run around to create the impression of a large cavalry force on the move. Another is the use of dummy missiles and fake artillery pieces in the 1991 Gulf War. In an attack on an information system, the attacker is apprised of the effects of his actions by the system responses. If a known virus is planted, then the deception could simulate the effects of the virus and lead the attacker to believe that his attack has been successful. The virus would then be removed without the knowledge of the attacker. If the attacker attempted a denial-of-service attack, the system could respond with a slowdown to simulate the success of the attack.

f. Demonstration

This refers to maneuvering one's forces with no intention of following through to distract or confuse the enemy. Sometimes demonstrations

are also conducted to desensitize the target to lull them into a false sense of security or complacency. Prior to the surprise Yom Kippur attack in 1973, the Egyptians moved their troops to conduct exercises near the border, and in the final exercise crossed the border into Israel [Dunnigan & Nofi, 1995]. Demonstrations in information systems may be counter-productive for the defender since a show of "strength" may invite rather than deter attackers. When Microsoft released their XP version of the Windows operating system as their "safest ever", hackers got to work on it almost immediately and soon found many flaws to exploit [Dunnigan, 2002]. A demonstration could work well in a honeypot, where attackers would unwittingly test their skills for the benefit of the honeypot's data collection.

g. Feints

Feints are an extension of a demonstration in that an attack is followed through. In so doing, the attacker distracts the enemy from the real main attack that is underway elsewhere. The classic example is the Allied invasion of Normandy in 1944, in which the Germans had been successfully misled to believe that the main attack would take place elsewhere. By the time the Germans discovered the truth, the Allies had already gained a strategic foothold on the French coast. In the cyber world, defensive feints may be carried out by blocking attacks on certain network ports with warning messages while allowing them on others where the effects of a successful attack may be simulated [Rowe & Rothstein, 2003].

h. Lies

Lies involve using media, messages or radio communications to falsely make pronouncements or answer enemy questions. Internet surfers may be greeted with annoying pop-up windows where a seemingly convenient link with the message "click here to close window" or spam mail with "click here to unsubscribe" actually connects them to sites where they are vulnerable to further attacks. The W32.Swen.A@mm worm and many of its variants send fake electronic mail messages that appear to have originated from Microsoft [Symantec, 2003].

i. Insight

Insight involves outthinking and outsmarting the enemy by seeing through his tactics and exposing his intent. Cyberwarfare is no different from conventional warfare in that the attackers and defenders can try to outsmart the opponent. Attacks typically include vulnerability scans, gaining access and administrator privileges, downloading malicious software and so on. It is possible to anticipate some of the attackers' moves through the use of a counterplan for deception [Rowe 2003], thereby creating an additional defensive layer against the attacker. Similarly, [Cohen2, 1998] used insight into the attackers' operations in his Deception Toolkit.

2. Semantic Cases

[Rowe, 2004] has developed a more comprehensive taxonomy of deception based on the theory of semantic cases. It is based on the claim that "deception operates on an action to change its perceived associated case values," and gives rise to many different methods of deception derived from a combination of cases. Out of the possible 30 cases, Rowe found that only 19 were amenable to application in information systems. Table 2 below lists the 19 cases and how they may apply in information systems.

Class	Case	Extension	Examples in Information Systems
Essence	Supertype	Generalization of the action type	Installing software with no purpose except to crash a computer
	Whole	Of which the action is a part	Changing the system-administrator password temporarily as part of an attack plan to steal secrets
Participant	Agent	Who initiates the action	Attacker pretends to be the system administrator
	Object	What the action is done to	Storing fake information on a computer system that you hope an attacker will steal
	Instrument	Something that helps accomplish the action	Putting spyware in a Web browser
Space	Direction	Of the action	Sending damaging cookies back to an attacker of a Web site
	Location-from		Spoofing of Internet IP address or Web pages
	Location-to		Attacks on unexpected sites or ports, like those of seemingly little value
	Location-through		Attacks through supposedly secure intermediate sites
Time	Frequency	Of occurrence	Denial of service created by overwhelming resources with transactions
	Time-at		False times for log file records
	Time-through		Deliberately delaying response to an attacker
Causality	Cause		Lying to an attacker about the network connection being down as the reason they cannot download something
	Effect		Lying to an attacker that a suspicious file has been downloaded
	Purpose		Software asking an attacker for their password to check whether it is good
Quality	Accompaniment	Additional object	A utility that contains a virus
	Content	Action object type	A file with an image-file extension that is actually an executable
	Measure	Quantity	Deliberately downloading a too-large file to create denial of service
	Value	transmitted	Deliberately capitalizing each command sent to a case-sensitive operating system

Table 2. A Selected List of Semantic Cases as Applied to Information Systems (After [Rowe, 2004]).

C. CYBER DECEPTION AND CYBER DEFENSE

Cyber deception is not employed for cyber attacks alone. Various groups of computer scientists and software engineers have developed cyber deception applications with a defensive slant. Some, like honeypots, are passive in nature and have a specific but limited purpose, while others like intelligent software decoys reinforce computer defense against cyber attacks.

1. Software Decoys

[Michael & Riehle, 2001] introduced intelligent software decoys to cover a "spectrum of deceptive defensive activity" in computers and networks. The goal of the software decoys is to provide additional layers of defense called software wrappers that divert the attention and resources of the attacker while giving the impression that the attack is succeeding. In so doing, the damage done to the target system is limited, while information on the attacker is being gathered at the same time.

The need for software decoys comes from the perceived ineffectiveness of existing protection methods. These include intrusion-detection systems (both anomaly and misuse detection), firewalls, and "patch-and-pray" methods [Rowe et al, 2002; Michael et al, 2002]. The problem is made worse by impending centralization of military information systems ("network-centric warfare") reinforcing the call for protection against cyber warfare [Michael, 2002]. Software decoys can be regarded as a viable second line of defense given the numerous vulnerabilities of COTS software and operating systems that are used by many military organizations.

Intelligent software decoys adapt to an intrusion instead of blocking it outright. Adapting refers to the ability to tolerate violations of the software contract which occurs when the "obligations and benefits between the component and the calling process or thread" are infringed [Michael, 2002]. At the same time, the intrusion is studied and diverted to an "antechamber" [Michael & Riehle, 2001] which may well reside on a different platform so as to limit the damage that could be inflicted by the attacker. Within this antechamber,

deception methods are applied to delay or distract the attacker, as shown by the examples in Table 2.

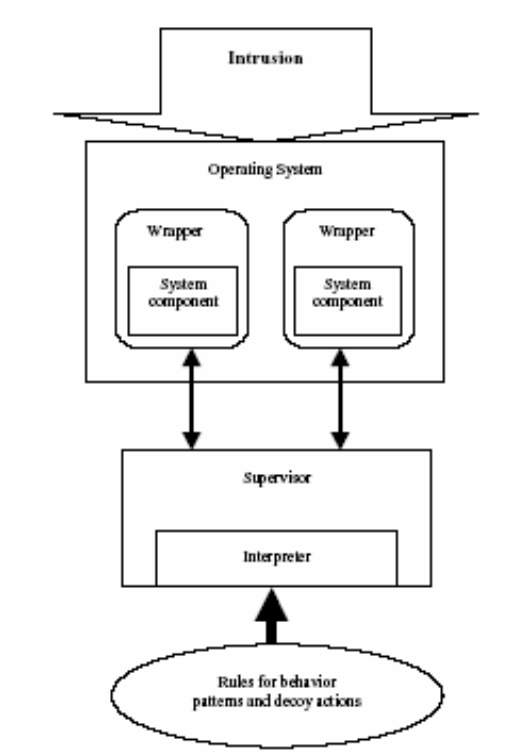

Figure 2. Software Decoy Architecture (From [Michael et al, 2002])

The software decoy architecture in Figure 2 shows the use of wrappers to protect software components against attack. The wrappers reside within the operating system and are supervised by predetermined rules that specify behavior patterns and decoy actions.

In a related development, [Rowe, 2004] suggested “generic excuses” that are based on his theory of deception from semantic cases. By making use of the human ability to derive patterns from what they observe or experience, the process of bundling together a series of deception ploys builds a hypothesis in the attacker’s mind. As a result, these generic excuses that are created from the bundle of deception ploys provide a potentially more convincing deception against attackers.

2. Other Related Work

The Deception ToolKit [Cohen2, 1998] was developed to "increase attacker workload while reducing defender workloads." It conveys an impression of the defenses of a computer system that are different from what they really are by creating phony vulnerabilities. The Deception ToolKit is effective against automated attack tools that scan for known vulnerabilities by reporting a large number of them, each with insufficient information to confirm them to be real or otherwise. This wastes the attacker's resources in having to test each one of them. In the meantime, each attack against the deceptive vulnerabilities is monitored. The Deception ToolKit raises two pertinent issues on deception. Firstly, it is difficult to create good deceptions to meet complex requirements, but simple deceptions that meet simple requirements are still useful as they can fool all but the most sophisticated attackers. Secondly, each failed attack against the deceptive vulnerabilities mentioned is immediately detected by the defender, giving the attacker little time to react and mount a successful attack thereafter. Given these, [Cohen2, 1998] concludes that there is indeed a very good case for using deception in cyber defense.

Honeypots [HoneyNet, 2002] were conceived to lure attackers to study their attack methods, patterns and techniques. A honeypot is a network of systems that is intended to be compromised by attackers to reveal their behavior during an attack. When the use of honeypots was revealed to the larger Internet community, hackers became more careful to look harder to see if the site they were attacking was in fact a honeypot. Some non-honeypot servers were also given honeypot-like features to deter those hackers who were familiar with such features [Dunnigan, 2002].

Recent work in the theory of cyber deception involves the use of deceptive agents in formalizing the decision to deceive [de Rosis et al, 2004]. The decision to deceive is part of a deception plan model that takes into account the dispositions, inclinations and mental states of the sender and receiver of the deception messages. This model explores the ability to deceive without having to lie, for example by conveying uninfluential truths to confuse the receiver, or by

exploiting the receiver's inherent distrust. The authors claim that the advantage of such "falsely sincere" deceptions are reduced risks and consequences of detection. Another aspect of the deception plan is the evaluation of the validity of a deception strategy to select the optimal deception instrument. The evaluation takes into consideration the impact, plausibility and credibility of the deception object, as well as its safety and computational costs. A final component in the evaluation is what the authors call the "horizon effect" which states that a good strategy is one that opens up good strategies in the future, as opposed to a strategy that is good now but turns bad later on. All the above are synthesized into a formal deception strategy and applied to a probability-based simulation experiment, in which the criteria applied by the system are evaluated against those applied by human subjects. However, there are risks associated with performing such experiments with human subjects, as their ability to deceive or be deceived varies with their backgrounds. There is also the issue of the "availability effect" in which people tend to assess the value of uncertainties heuristically to size the situation better, and this sometimes leads to systematic errors.

D. PITFALLS OF CYBER DECEPTION

As with conventional deception, there are cyber traps that can backfire, or forms of cyber deception that are inherently riskier than others. The use of cyber deception could irritate genuine users who have legitimate rights to the system, only to find that the attempt to gain access to a certain directory within the system has led them down a different, unexpected path. Imagine the annoyance if a user had spent time and effort working on a document and tried to save it in a particular directory, only to find that it has gone missing because the directory was a deceptive one [Rowe & Rothstein, 2003].

When cyber deception is employed against hackers, the effects could vary depending on the nature of the attack. An amateur or script kiddie may be put off by the lack of success and move on to another system, in which case the defense was successful. If the deception was detected, they could be provoked

and see it as a challenge. That would lead them to try harder using alternative methods to defeat the defenses. In addition to the risk of being detection, [de Rosis et al, 2004] also considers the severity of the consequence of the detection, and both risk and consequence are grouped together as a "safety" factor in their calculations. A professional hacker who is targeting a particular system may not be deterred and may simply be angered by the discovery of having been fooled by the deception. A terrorist may revert to conventional means of physical attack if cyber attacks are unsuccessful. The use of cyber deception may also introduce unintended consequences. When deception was employed to counter computer network scanners, it also worked against genuine users. The same technology used to keep out unwanted scanners was also successful against bona fide workers who were scanning their systems for vulnerabilities [Cohen2, 2001].

E. CYBERTERRORISTS AND CYBER DECEPTION

1. Attack Tools

As many of the offensive operations that a cyberterrorist would carry out involve attacking information systems, we can expect that many of the attack tools employed by the cyberterrorist will be the same as those used by cyber activists, hackers, and cyber criminals.

[Cohen3, 1998] postulated that the three main aspects of information technology exploited by cyberterrorists are anonymity, cryptography, and the widespread release of attack tools. Anonymity enables the cyberterrorists to carry out their tasks without fear of reprisals, since true anonymity means that their identity cannot be traced and exposed. Cryptography reinforces anonymity but also provides cyberterrorists with security and confidentiality of their communications from law enforcement agencies. Since the release of high-quality cryptography such as Pretty Good Privacy (PGP) to the public, cryptography has been a double-edged sword as it can serve both good and evil purposes; [Denning, 1995] mentioned a report by the FBI on the use of encryption by terrorists who were plotting to assassinate Pope John Paul II

during his visit to the Philippines. The third issue, the release of attack tools over the Internet, may actually enhance security by providing useful information about attacks to law enforcement as well as providing tools to defenders for searching their own systems for vulnerabilities [Dunnigan, 2002]. The flip side of the coin, as argued by Cohen, is that with so much information and data available, military intelligence or law-enforcement agencies will have a much harder time trying to sift through the noise to expose the real cyberterrorist attacks.

Other cyber attack tools provide the means for attackers to achieve their goals in cyberspace. There are roughly four categories, namely reconnaissance, scanning, gaining access and maintaining access. Table 3 below provides a brief description and some generic examples.

Attack Step	Description	Examples
Reconnaissance	Obtaining information on the target by researching the Web, newsgroups, open source media or actively seeking the information through unscrupulous means.	- Desk checking - Social engineering - Dumpster diving - Physical break-ins
Scanning	Searching for vulnerable servers or personal computers that are connected to the Internet.	- Network mapping - Port scanning - Vulnerability scanning
Gaining Access	Obtaining entry to a vulnerable computer by exploiting weakness or flaws in its operating system, or through the use of access controls that were fraudulently retrieved.	- Stack-based buffer overflow attacks - Password attacks - Password cracking tools - Sniffing - IP address spoofing - Session hijacking
Maintaining Access	Taking steps to avoid being discovered or planting malicious software so as to be able to regain access to the target system	- Covering tracks - Backdoors and Trojan Horses - Keystroke loggers - Rootkits

Table 3. Cyberterrorism Techniques (After [Denning1, 1999; Dunnigan, 2002; Fox et al, 2002]).

Using the attack steps in Table 3 and Cohen's list of attack mechanisms [Cohen1, 1998], we find that most of the software-based attack mechanisms

apply to gaining and maintaining access. As such, we will concentrate on these two steps. These are listed in Table 4.

Target	Attack Technique	Desired Effect	Difficulty
Information Systems	Denial-of-service	System non-availability	Easy
	Rootkit installation	Control of system	Moderate
	Sabotage	System manipulation / destruction	Easy
	Trojan Horse	Control of system / system destruction	Moderate
	Buffer overflow attack	Control of system	Moderate
	Spoofing	Control of system	Moderate
	Password theft / attack	Control of system	Easy
	Virus / worm	System non-availability / destruction	Easy
	Data diddling	System non-availability / manipulation	Moderate
	Subversion	Control of system	Hard
Web sites	Denial-of-service	Site non-availability	Easy
	Defacement	Hacktivism	Easy
		Terror	
	Virus / worm	Site non-availability / destruction	Moderate
Electronic Mail	Denial-of-service	Service non-availability	Easy
	Rumor spreading	Propaganda	Easy
		Deception	
	Virus / worm	Service non-availability / destruction	Moderate
General public	Extortion (e.g. by publishing on Web site names of police officers targeted for attack)	Fear	Moderate

Table 4. Cyberterrorism Attack Tools (After [Cohen1, 1998; Denning1, 1999]).

We find that in most instances, carrying out the attacks is not hard. The main reason for this is that there is a plethora of existing attack tools which can be easily downloaded from the Internet, and the list is increasing every day. The

findings from the 1997 no-notice exercise ELIGIBLE RECEIVER stated that there were some 1900 Web sites from which hacking tools were publicly available. There could be many more today. The ease of attack applies not only to target Web sites and electronic mail, but also to information systems such as electronic commerce or database systems. Moreover, it should be mentioned that the reconnaissance and scanning steps are also relatively easy to carry out. In particular, there are also many automated tools widely available on the Internet for scanning. On the whole, we find that the apparent ease with which a cyberterrorist may attack suggests that it is a question of the will of cyberterrorists, and not the feasibility, that prevents them from actually attacking.

2. Terrorists, Cyberterrorists, and Deception

[Cohen3, 1998] postulates that terrorist tactics are deceptive in nature because the sense of fear that they create is larger than the danger they actually pose. To use Whaley's terminology, terrorism is mimicking a threat that is grossly exaggerated, while masking the terrorists' true capabilities in imposing a danger to warrant that level of threat. In cyberspace, a similar level of fear could be generated if an act of cyberterrorism like those mentioned previously occurs. For one, it could be unprecedented, and this alone would generate a significant amount of publicity. The media could quickly become a proxy tool of the cyberterrorists as different publications vie to postulate the vulnerabilities of information systems to cyberterrorists, the failure of government to prevent such an event, and the likely occurrence of copycat acts. A September 2003 Washington Post article cited a Pew study in which nearly half of the 1000 Americans surveyed feared that the next terrorist attack would involve a cyber component [McCarthy, 2003]. Given our heavy reliance on information technology, a solitary act by one cyberterrorist group could have political and psychological ramifications beyond the actual act. However, until we see such an event, many are still swayed by the arguments of the "cry wolf" and "realist" camps, and will continue to regard cyber attacks as a costly nuisance.

[Higginbotham, 2001] explored several ways in which terrorists may themselves be deceived. First, many of these organizations have a patriarchal

structure with followers of fanatical and unquestioning loyalty. This combination suggests that targeting the terrorist leadership alone could have a significant effect on the entire organization. Second, to operate effectively, terrorists need accurate intelligence. In addition to the traditional sources of intelligence such as the media, terrorists are increasingly reliant on the Internet and information technology to meet their intelligence requirements [Cohen3, 1998]. These create new channels through which they can also be deceived. Third, terrorists constantly strive to balance between operational efficiency and security. High levels of security drastically impede their ability to carry out operations. Conversely, being able to conduct their operations efficiently usually comes at a cost to security and secrecy. Deception operations could be targeted at the terrorist organizations' confidence in their own security to affect their operational efficiency.

The future of terrorism sees in part a trend towards human networks, with loose organizations working in small groups and held together by a common purpose. Their command-and-control is dispersed but they are connected via the Internet and other communications technologies. One implication of network organizations is that there is no single center of gravity which if targeted would disable the entire terrorist group. Another implication is their ability to operate across national boundaries, making it difficult for any one country to effectively deal with them. However, their dispersion also creates weaknesses, since the constant need for communications and coordination in the network exposes them to vulnerabilities of interception and eavesdropping. If they use electronic mail, which they likely are, they are also exposed to tracing, surveillance and cyber attacks [Higginbotham, 2001; Arquilla & Ronfeldt, 2001].

How such networked organizations may benefit cyberterrorist groups remains to be seen. One may argue that it is the technology-savvy groups that have brought about such a revolution to the structure of terrorist organizations in the first place. Given their track record and credentials for violence, these may be the groups that are most likely to build a cyberterrorism capability that they are prepared to use. Conversely, cyberterrorism requires a high level of expertise.

For a cyberterrorist group to operate effectively, it will likely need to centralize its computer experts and equipment. Some organizations may incorporate both features, with a networked structure to support the “traditional” terrorist activities, and a cyberterrorist wing where cyber attack capabilities are developed and implemented. Such a dual structure is difficult to deceive. The weaknesses of the networked structure are not present in a centralized cyberterrorist wing; yet the cyberterrorist wing cannot be influenced by targeting its leadership because the terrorist leader is apart from the wing itself.

Combining these factors with the actors elaborated in Chapter II, we can explore the possibilities for deception. Table 5 on the next page shows the four ways in which terrorists may be deceived in a matrix against the six categories of cyberterrorists (expanded from the four in Chapter II for greater granularity). The possible outcomes have been shaded for clarity.

Deception Target / Actors	Leadership	Cyberspace intelligence	Security confidence	Communication networks
a. Lone cyberterrorists	Possible: Brains and body are one and the same	Possible: The Internet is likely a major source of intelligence	Difficult: They do not need to trust others	Difficult: No need for communications
b. Small, technologically sophisticated groups	Possible: Leader has direct control of organization	Possible: The Internet is likely a major source of intelligence	Difficult: Group cohesion expected to be tight	Difficult: Being small and centralized reduces communication requirements
c. Same as b. but as a wing in a larger organization	Difficult: Group leader different from organization leader	Possible: The Internet is likely a major source of intelligence	Difficult: Group cohesion could be tight but it is not certain	Difficult: Being small and centralized reduces communication requirements
d. Large Religious fundamentalist organizations	Possible: Leader has direct control of organization	Possible: The Internet is likely a major source of intelligence	Possible: Large organizations cannot have complete control over information flows	Possible: Large dispersed organizations need frequent communications for coordination
e. Government-backed or sponsored units	Possible: Group leader may be known	Difficult: They would have ready access to other intelligence sources	Difficult: Secrecy and security not a fear-inducing issue	Possible: Large dispersed organizations need frequent communications for coordination
f. Same as e. but government links are covert	Difficult: Hierarchy of leadership not easy to determine	Difficult: They would have ready access to other intelligence sources	Difficult: Secrecy and security not a fear-inducing issue	Difficult: Need for additional secrecy would probably result in special communications means

Table 5. Deceptions against Cyberterrorists.

Table 5 suggests that many of the cyberterrorist categories are susceptible to deceptions in cyberspace. This is probably due to their heavy reliance on it for their medium of operations. The table also suggests that government cyberwarfare units could be difficult to deceive, because they are not in the same outlaw situation as terrorists. A further conclusion that we can draw

from Table 5 as well as from many examples earlier in this chapter is that cyberspace offers significant opportunities for deceiving cyberterrorists. It remains to be shown that cyber deception is a viable defense against the attacks of cyberterrorists.

[Rowe and Rothstein, 2003] concluded that only lies, displays and insights from Dunnigan and Nofi's taxonomy of deception [Dunnigan & Nofi, 1995] were suitable as tools for defensive deception. Combining these with Rowe's generic excuses [Rowe, 2004] and the attack stages (Table 3), we can explore the viability of cyber deception against the different stages of a cyber attack. These are elaborated in Table 6 below. The viable outcomes are shaded for clarity.

Deception Target / **Attack Stages**	**Generic Excuses / Lies** (e.g. false error messages)	**Displays** (e.g. simulating attack effects)	**Insight** (e.g. deception counterplan)
Reconnaissance	Web searches could be turned away	Not applicable, since there is no attack	Difficult to tell between legitimate network monitoring and others
Scanning	Automated scanners may be fooled	Not applicable, since there is no attack	Difficult to tell intention of scanner
Gaining Access	Attacker could be frustrated and try other approaches	Attacker could be fooled by apparent success	Attacker could be exposed and diverted to antechamber
Maintaining Access	Attacker could be frustrated and give up	Attacker assumes he is successful	Attacker assumes he is successful

Table 6. Cyber Deceptions and Cyber Attacks

We see that cyber deceptions have limited success in trying to thwart reconnaissance and scanning efforts. In any case, we should not be trying to deceive every attempt to reconnoiter or scan our systems as we are still unsure of their intentions. However, our intrusion-detection systems should now be on the alert and ever watchful of attempts to move to the next step. By attempting to gain unauthorized access, we would have ascertained that an attack is taking

place and this is where cyber deception can be effective. Although Table 6 only deals with generic examples, it is clear that cyber deception can be an effective second line of defense [Michael & Riehle, 2001; Rowe et al, 2002] when the attacker is attempting to gain access, or has already done so.

V. CONCLUSION

While there have been many studies in the separate areas of terrorism, cyberterrorism, deception and cyber warfare, it is hoped that by putting them together we can establish the significance of the cyberterrorism threat. We have verified firstly that cyberterrorists are likely to have similar motivations with terrorists in desiring violence and destruction to meet their political or other causes. While there have been no clear acts of cyberterrorism to date, this could be the result of lack of motivation or ability to carry out the attacks in cyberspace and not the feasibility. However, this situation is not expected to remain as is, given the advantages offered by cyberterrorism against forces and societies that rely heavily on information technology. Moreover, many terrorist and state sponsored groups are seeing the asymmetrical benefits of information warfare as a means of redressing the conventional military imbalance of the U.S. vis-à-vis the rest of the world.

Secondly, we see that deception has been commonplace in nature and in human history, and it has quickly pervaded cyberspace as an offensive tool. Unfortunately, many of the existing uses of cyber deception have tended to be for unethical or immoral purposes. If employed innovatively and skillfully, cyber deception could become an essential component of defense mechanisms in future. Many such deception ideas have been proposed.

Thirdly, if it is possible to deceive terrorists, then it should also be possible to deceive cyberterrorists. The reliance of cyberterrorists on information technology makes them vulnerable to cyber deceptions. In addition, many of the methods and tools that cyberterrorists would use are similar to those used by other less malicious hackers, so we can plan specific deceptions to use against them in advance.

Finally, the lack of actual examples of cyberterrorism (although a blessing) makes it hard to pinpoint specific methods, tools or desired outcomes for policy recommendations. There is much literature available on the methods,

motivations and psychology of terrorists, but little is available in comparison for cyberterrorists. What is available tends to be confined to arguments on the nature of the threat, rather than the threat itself. Thus more work will need to be done on studying the vulnerability of critical information systems, their potential exposure to cyberterrorists and the damage they could do if they gained access. Finally, just like updating an anti-virus software against new strains of viruses, cyber deception methods that are being developed need to be constantly updated to remain relevant in their ability to deceive a cyberterrorist attack.

LIST OF REFERENCES

[Anderson, 2002]
Emory A. Anderson III. *A Demonstration of the subversion threat: Facing a critical responsibility in the defense of cyberspace*. M.S. in Computer Science 2002, Naval Postgraduate School, Monterey CA. http://library.nps.navy.mil/uhtbin/hyperion-image/02Mar_AndersonE.pdf, accessed October 2003.

[Armstrong, 2002]
Illena Armstrong. *Hactivism: Protest or Petty Vandalism?* Special Feature, September 2002. http://www.scmagazine.com, accessed August 2003.

[Armstrong, 2003]
Illena Armstrong. *Real Risk or Shadow? The Threat of Cyberterrorism*. Articles and Features, January 2003. http://www.scmagazine.com, accessed August 2003.

[Arquilla & Ronfeldt, 2001]
J. Arquilla & D. Ronfeldt, (Eds). *Networks and Netwars: The Future of Terror, Crime, and Militancy*. Santa Monica, CA: RAND, 2001.

[Ashley, 2003]
Bradley K. Ashley, Lt. Col, USAF. *Anatomy of Cyberterrorism: Is America Vulnerable?* Research Paper, Air War College, Air University, Maxwell AFB, AL. 27 February 2003.

[Bell & Whaley, 1991]
J. Bowyer Bell and Baron Whaley. *Cheating and Deception*. New Jersey: Transaction Publishers 1991.

[Betts, 2002]
Richard K. Betts. *Fixing Intelligence*. Foreign Affairs, January/February 2002.

[Burgess, 2003]
Mark Burgess. A Brief History of Terrorism. The Center for Defense Information, July 2003. http://www.cdi.org/terrorism, accessed October 2003.

[Carr, 2000]
C. Carr (Ed). *The Book of War*. New York: Random House. 2000.

[CERT, 2003]
Computer Emergency Response Team Coordination Center (CERT / CC) Statistics 1988-2003. http://www.cert.org/stats/cert_stats.html, accessed November 2003.

[Cohen1, 1998]
Frederick B. Cohen, Dr. *A Preliminary Classification Scheme for Information System Threats, Attacks and Defenses*. Sandia National Laboratories, September 1998. http://all.net/journal/ntb/cause-and-effect.html, accessed September 2003.

[Cohen2, 1998]
Frederick B. Cohen, Dr. *A Note on the Role of Deception in Information Protection*, 1998 http://all.net/journal/deception/deception.html, accessed September 2003.

[Cohen3, 1998]
Frederick B. Cohen, Dr. *Deception and Perception Management in Cyber-Terrorism*, 1998 http://all.net/journal/deception/terror-pm.html, accessed September 2003.

[Cohen2, 2001]
Frederick B. Cohen, Dr. *A Framework for Deception*. Technical Baseline Report, Nov 2001. http://all.net/journal/deception/Framework/Framework.html, accessed September 2003

[Cohen, 2002]
Frederick B. Cohen, Dr. *Deception Rising*. Managing Network Security series, Sep 2002. http://all.net/journal/netsec/2001-11.html, accessed September 2003.

[Crenshaw, 1981]
Martha Crenshaw. *The Causes of Terrorism*. Comparative Politics, pp381-385. July 1981

[Crenshaw, 1995]
Martha Crenshaw. *Terrorism in Context*. Pennsylvania State University Press. 1995

[CSIS, 1998]
CSIS Task Force Report. *Cybercrime… Cyberterrorism… Cyberwarfare… Averting an Electronic Waterloo*. Washington D.C.: Center for Strategic and International Studies, 1998.

[CSIS, 2001]
CSIS Report. *Cyber Threats and Information Security: Meeting the 21st Century Challenge*. A report for the CSIS Homeland Defense Project. Washington D.C.: Center for Strategic and International Studies, May 2001.

[Denning, 1995]
Dorothy E. Denning. *The Future of Cryptography*. Internet Security Review, October 1995.

[Denning1, 1999]
Dorothy E. Denning. *Information Warfare and Security*. New York: ACM Press 1999.

[Denning1, 2000]
Dorothy E. Denning. *Cyberterrorism.* Global Dialogue, Autumn 2000. http://www.cs.georgetown.edu/~denning/infosec/cyberterror-GD.doc, accessed July 2003.

[Denning2, 2000]
Dorothy E. Denning. *Cyberterrorism.* Testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services, US House of Representatives, May 23, 2000. http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html, accessed July 2003.

[Denning, 2001]
Dorothy E. Denning. *Is Cyber Terror Next?* Georgetown University, November 2001. http://www.ssrc.org/sept11/essays/denning.htm, accessed July 2003

[de Rosis et al, 2004]
Fiorella de Rosis, Cristiano Castelfranchi, Valeria Carofiglio and Giuseppe Grassano. *Can Computers Deliberately Deceive? A Simulation Tool and its Application to Turing's Imitation Game*. Computational Intelligence, to appear 2004.

[Devost, 1995]
Matthew G. Devost. *Hackers as a National Resource*. Information Warfare – Cyberterrorism: Protecting Your Personal Security in the Electronic Age. Winn Schwartau (Ed). Second Trade Paperback Edition. New York: Thunder's Mouth Press, 1996.

[Devost et al, 1996]
Matthew G. Devost, Brian K. Houghton & Neal A. Pollard. *Information Terrorism: Can You Trust Your Toaster?* The Terrorism Research Center, 13 April 1996. www.terrorism.com, accessed August 2003.

[Dunnigan & Nofi, 1995]
James F. Dunnigan & Albert A. Nofi. *Victory and Deceit: Dirty Tricks at War*. William Morrow and Co. 1995.

[Dunnigan, 2002]
James F. Dunnigan. *The Next War Zone: Confronting the Global Threat of Cyberterrorism*. New York: Citadel Press Books, 2002.

[Fowler & Nesbi, 1995]
Charles A. Fowler & Robert F. Nesbit. *Tactical Deception in Air-Land Warfare*. Journal of Electronic Defense. June 1995

[Gerwehr & Russell, 2000]
Scott Gerwehr and Glenn W. Russell. The Art of Darkness: Deception and Urban Operations. RAND 2000.

[Gerwehr & Russell, 2002]
Scott Gerwehr and Glenn W. Russell. *Unweaving the Web: Deception and Adaptation in Future Urban Operations*. RAND 2002.

[Gordon & Ford, 2002]
Sarah Gordon and Richard Ford. Cyberterrorism? Symantec Security Response White Paper 2002.

[Higginbotham, 2001]
Benjamin I. Higginbotham. *On Deceiving Terrorists*. M.S. in Defense Analysis 2001, Naval Postgraduate School, Monterey CA. http://library.nps.navy.mil/uhtbin/hyperion-image/01Dec_Higginbotham.pdf, accessed September 2003.

[Hoffman, 1999]
Bruce Hoffman. *Inside Terrorism*. Paperback Edition, London: Indigo 1999.

[HoneyNet, 2002]
The HoneyNet Project. *Know your enemy*. Boston: Addison-Wesley, 2002.

[IWS, 2003]
IWS – The Information Warfare Site. *Annual Report On The Military Power Of The People's Republic Of China*. 28 July 2003. http://www.iwar.org.uk/iwar/resources/news/china-io-2003.htm, accessed December 2003.

[Joint, 1995]
Joint Chiefs of Staff, JCS Pub 1-02, March 1995.

[Joint, 1996]
Joint Doctrine for Military Deception, Joint Pub 3-58, 31 May 1996.

[Jones, 1989]
R.V. Jones, Dr. *Reflections on Intelligence*. London: William Heinemann Ltd., 1989.

[Kam, 1988]
Ephraim Kam. *Surprise Attack: The Victim's Perspective*. Massachusetts: Harvard University Press, 1988.

[Krautwurst, 2001]
Terry Krautwurst. *Jokers of the Wild*. National Geographic World Magazine. National Geographic Society. April 2001.

[Lang, 2002]
Dave Lang. *Cyberterrorism*. SC Infosec Opinionwire. February 2002.

[Leyden, 2003]
Joel Leyden. *Al-Qaeda : The 39 principles of Holy War*. Israel News Agency. 4 September 2003

[Love, 2003]
David Love. *Is Cyberterrorism a Serious Threat to Commercial Organizations?* SC Infosec Opinionwire. February 2003.

[McCarthy, 2003]
Ellen McCarthy. *Americans Fear Cyberattacks from Terrorists, Study Shows*. The Washington Post. Washington D.C.: September 3, 2003.

[Michael & Riehle, 2001]
James B. Michael and Richard D. Riehle. *Intelligent Software Decoys*. Proceedings of the Monterey Workshop: Engineering Automation for Software Intensive System Integration, Monterey California. Pp 178-187. June 2001.

[Michael, 2002]
James B. Michael. *On the Response Policy of Software Decoys: Conducting Software-Based Deception in the Cyber Battlespace*. Proceedings of the 26th Annual International Computer Software and Applications Conference (COMPSAC '02), IEEE, 2002.

[Mitnick, 2002]
Kevin D. Mitnick. *The Art of Deception: Controlling the Human Element of Security*. Indianapolis: Wiley Publishing 2002.

[NPS, 1999]
Naval Postgraduate School White Paper. *Cyberterror: Prospects and Implications*. Center for the Study of Terrorism and Irregular Warfare, NPS, Monterey CA. December 1999.

[Ollmann, 2003]
Gunter Ollmann. The Fine Art of Deception. Articles and Features, August 2003. http://www.scmagazine.com, accessed September 2003.

[Post, 1998]
Jerrold M. Post. *Terrorist Psycho-logic: Terrorist behavior as a product of psychological forces*. Origins of Terrorism, Walter Reich (Ed). Baltimore: John Hopkins University Press. 1998.

[Reich, 1998]
Walter Reich. *Understanding Terrorist Behavior*. Origins of Terrorism, Walter Reich (Ed). Baltimore: John Hopkins University Press. 1998.

[Rodgers, 2003]
Paul Rodgers. *Protecting America Against Cyberterrorism*. U.S. Foreign Policy Agenda. Volume 6, Number 3, November 2001

[Rowe, 2003]
Neil C. Rowe. *Counterplanning Deceptions to Foil Cyber-Attack Plans*. Proceedings of the 2003 IEEE Workshop in Information Assurance, West Point, New York, June 2003.
http://www.cs.nps.navy.mil/people/faculty/rowe/iacounter.htm, accessed July 2003.

[Rowe & Rothstein, 2003]
Neil C. Rowe & Hy Rothstein. *Deception for Defense of Information Systems: Analogies from Conventional Warfare*. Departments of Computer Science and Defense Analysis, U.S. Naval Postgraduate School, January 2003. http://www.cs.nps.navy.mil/people/faculty/rowe/mildec.htm, accessed October 2003.

[Rowe, 2004]
Neil C. Rowe. A Theory of Deception during Cyber-Attacks on Information Systems. Department of Computer Science, U.S. Naval Postgraduate School, in press, to appear 2004.

[Shulsky & Schmitt, 2002]
Abram N. Shulsky & Gary J. Schmitt. *Silent Warfare: Understanding the World of Intelligence*. Washington D.C.: Brassey's Inc. Third Edition, 2002.

[Skoudis, 2002]
Edward Skoudis. *The Hack Counter-Hack Training Course*. Prentice Hall PTR. 2002.

[STI, 2003]
Straits Times Interactive. Thwarting the Cyber Terrorist. Article by Ho Kar Wei and Ben Nadarajan, Nov 13, 2003. http://www.straitstimes.com.sg/singapore/story/0,4386,219807,00.html, accessed 14 November 2003.

[Sullivan, 2002]
Bob Sullivan reporting for MSNBC. *Is a Larger Net Attack on the way?* October 2002 http://www.msnbc.com/news/827209.asp?cp1=1, accessed October 2003.

[Sullivan, 2003]
Bob Sullivan reporting for MSNBC. *Fake FBI site tries to lure victims*. Sep 2003. www.msnbc.com/news/974015.asp?cp1=1, accessed October 2003.

[Symantec, 2003]
Symantec Security Response Newsletter, Oct 2003. http://securityresponse.symantec.com, accessed November 2003.

[Thomas, 2003]
Timothy L. Thomas. *Al Qaeda and the Internet: The Danger of "Cyberplanning"*. Parameters. Spring 2003.

[Tullett, 2003]
Jon Tullett. *Crying Wolf on Cyberterrorism?* SC Infosec Opinionwire. February 2003.

[Verstappen, 2003]
Stefan Verstappen. *The Thirty-Six Strategies of Ancient China.* San Francisco: China Books & Periodicals, 1999.

[Waltz, 1998]
Edward Waltz. *Information Warfare: Principles and Operations*. Massachusetts: Artech House, Inc., 1998.

[Whaley, 1980]
Barton Whaley. *Deception – Its Decline and Revival in International Conflict*. Propaganda and Communication in World History, Vol II. Harold D. Lasswell, Daniel Lerner, Hans Speier (editors). Honolulu: The University Press of Hawaii, pp 339-367. 1980.

[Whaley, 1982]
Barton Whaley. *Toward a General Theory of Deception*. The Journal of Strategic Studies, Vol. 5, No. 1, pp 178-192. March 1982.

[Whaley, 1987]
Barton Whaley. *When Deception Fails: The Theory of Outs*. Draft 1987.

[Whittaker, 2001]
David J. Whittaker (Ed.) *The Terrorism Reader*. New York: Routledge 2001.

[Wired News, 2002]
Wired News. *Servers Bounce Back from E-Attack*. Associated Press report Oct 22, 2002. http://www.wired.com/news/politics/0,1283,55957,00.html, accessed November 2003.

[Yam, 2001]
Jovi Tanada Yam. *Bracing for cyberwar*. BusinessWorld Publishing Corporation. 4 October 2001.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Director TDSI
   Temasek Defence Systems Institute
   Singapore

4. Neil C. Rowe
   Naval Postgraduate School
   Monterey, California

5. Dorothy E. Denning
   Naval Postgraduate School
   Monterey, California